Guide to the Azure Active Directory Best Practices Checklist

This resource corresponds to the **Microsoft 365 Azure AD Best Practices Checklist** spreadsheet, which is intended to be used as a baseline for provisioning new Microsoft 365 tenants according to best practices. The Spreadsheet is updated frequently so please try to get the most updated version. The selections have been made carefully, to apply to all levels of the Microsoft 365 suite.

© Copyright 2019-2022, Azure AD

AZURE AD

1

© Copyright 2019-2022, Azure AD

AZURE AD

2

Table of Contents

[Guide to the Azure Active Directory Best Practices Checklist](#_bookmark0) [1](#_bookmark0)

[Items of Critical Importance](#_bookmark1) [4](#_bookmark1)

* [Create emergency access global admin accounts](#_bookmark2) [4](#_bookmark2)
* [Use RBAC roles to limit admin privileges](#_bookmark3) [5](#_bookmark3)
* [Configure Multi-factor authentication & combined registration](#_bookmark4) [6](#_bookmark4)
* [Set up Conditional access according to Best Practices](#_bookmark5) [10](#_bookmark5)
* [Enable Temporary Access Pass (TAP)](#_bookmark6) [12](#_bookmark6)
* [Configure device settings for Azure AD joined devices](#_bookmark7) [12](#_bookmark7)
* [Configure the password expiration policy](#_bookmark8) [15](#_bookmark8)

[Items of Recommended Importance](#_bookmark9) [17](#_bookmark9)

* [Enable Self-service password reset (SSPR)](#_bookmark10) [17](#_bookmark10)
* [Follow best practices for security groups](#_bookmark11) [19](#_bookmark11)
* [Restrict Azure AD Join and Auto-enrollment](#_bookmark12) [21](#_bookmark12)
* [Restrict user access and app registration in Azure AD](#_bookmark13) [23](#_bookmark13)
* [Manage application consent and permissions](#_bookmark14) [24](#_bookmark14)

[Option 1. Disable app consent](#_bookmark15) [25](#_bookmark15)

[Option 2. Limit app consent](#_bookmark16) [26](#_bookmark16)

[Option 3. Admin consent request workflow](#_bookmark17) [28](#_bookmark17)

* [Restrict guest access and configure external collaboration](#_bookmark18) [31](#_bookmark18)
* [Trust claims from other Azure AD tenants](#_bookmark19) [33](#_bookmark19)
* [Configure SSO for Enterprise applications](#_bookmark20) [34](#_bookmark20)

[Items of Optional Importance](#_bookmark21) [39](#_bookmark21)

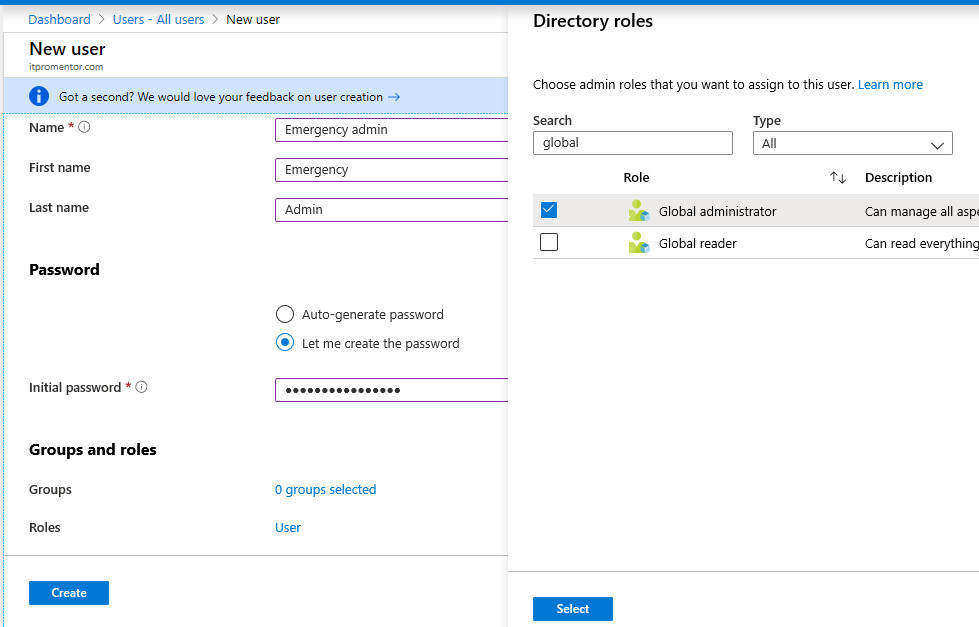
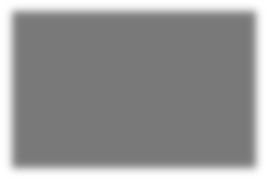
* [Configure Company branding](#_bookmark22) [39](#_bookmark22)
* [Enable Directory level timeout for the Azure portal](#_bookmark23) [42](#_bookmark23)
* [Use Administrative Units to delegate admin permissions](#_bookmark24) [42](#_bookmark24)
* [Considerations for Hybrid Azure AD Join](#_bookmark25) [43](#_bookmark25)
* [Azure AD Premium P2 features](#_bookmark26) [44](#_bookmark26)

[Conclusion](#_bookmark27) [45](#_bookmark27)

© Copyright 2019-2022, Azure AD

AZURE AD

3



Items of Critical Importance

* Create emergency access global admin accounts

[Microsoft recommends](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access) leaving two emergency access or “break glass” admin accounts, one excluded from each: MFA, and Conditional access policies. Go to **Users > New user**.

Assign name & username (use the “onmicrosoft.com” domain). Pick **Roles** and find the **Global administrator**. **Create** the account, noting the temporary password.

Login using the temporary password. Make sure to reset the password using a very long character string, such as 100 characters or more, randomly generated. The maximum password character length is 256.

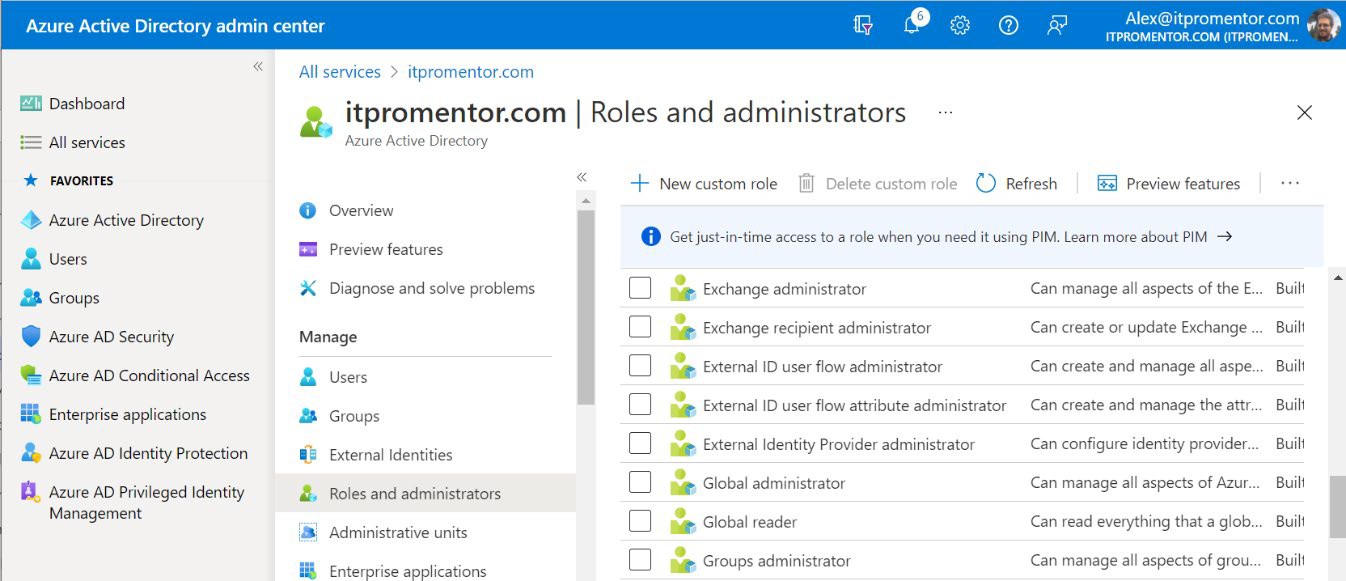
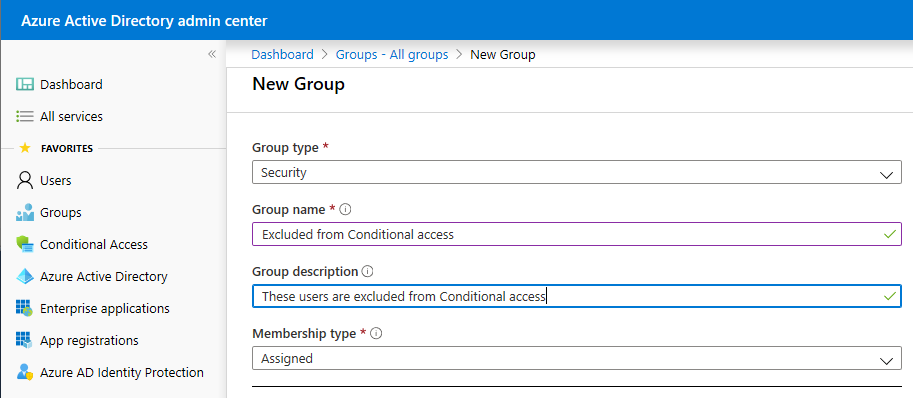
also recommend creating a security group called “Exclude from CA” or similar and adding one account to that group, then assigning that group to the “Exclude” tab of every Conditional access policy. Anyone else who needs to be excluded from CA can be added or removed from the group easily, as needed. Be sure to review other guidance about these accounts on

[Microsoft’s docs article.](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access)

© Copyright 2019-2022, Azure AD

AZURE AD

4



* Use RBAC roles to limit admin privileges

Do not give out **Global administrator** to every single person who needs to perform administrative tasks. For example, you can delegate specific roles like **Billing administrator**, **Helpdesk administrator**, or **License administrator**. If you have a service account that performs a task like backup or monitoring, then you can use the built-in Azure AD role **Global reader**, to limit access to read-only operations. Global reader is like a “read-only” version of Global admin.

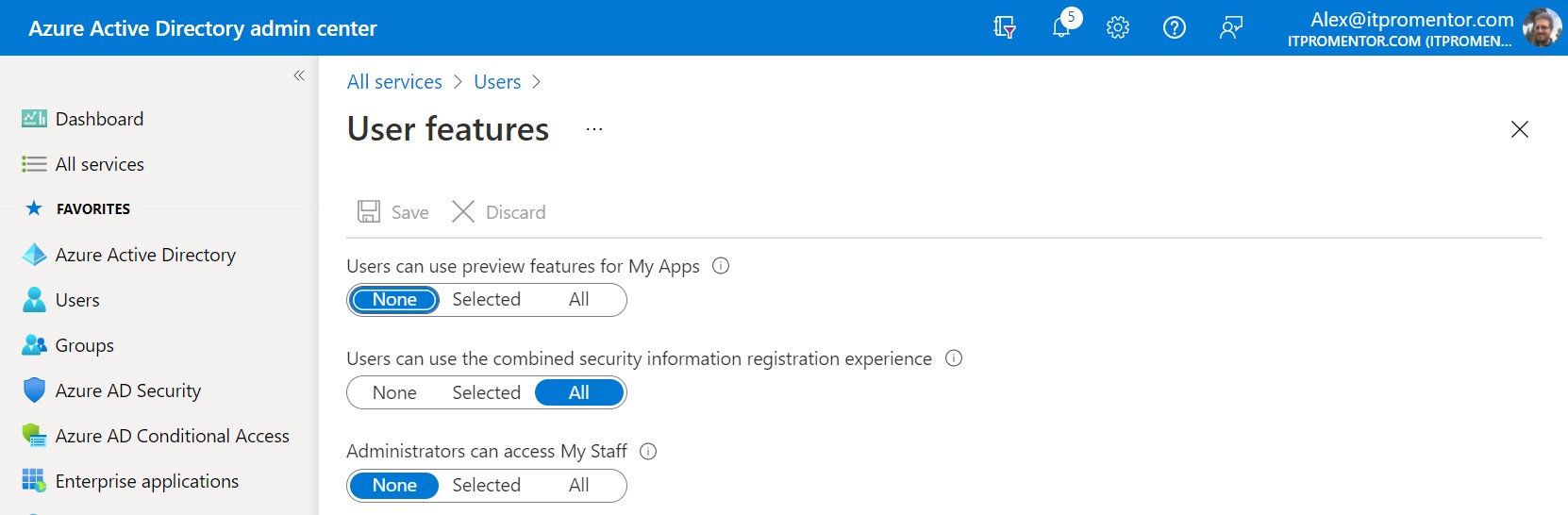
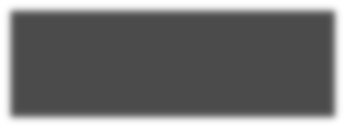
Find roles under **Azure AD > Roles and administrators**.

Select the role to add assignments as needed.

© Copyright 2019-2022, Azure AD

AZURE AD

5



* Configure Multi-factor authentication & combined registration

In Microsoft 365, we have a few different flavors of MFA, summarized in the following table.

*Note: You should avoid mixing the “per-user” MFA with Conditional Access or the Security Defaults feature. You should only use one method.*

Before enabling multi-factor authentication via any method, check to make sure that your tenant is enabled for the [combined registration](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined) experience. This should be on by default for new

tenants, but some older ones may still need to be switched over manually.

© Copyright 2019-2022, Azure AD

AZURE AD

6

Find this option under

**Users > User settings > Manage user feature settings**

**Method Description How to enable**

[**Security Defaults**](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults)

Enabled by default for new tenants. Blocks basic authentication, Requires MFA for admin accounts, requires users to register for MFA and applies account protection.

Azure AD > Properties > Manage Security Defaults

[**Conditional Access**](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access#common-policies) **(preferred)**

Custom security policies that apply access controls based on factors like device state, location, and client application. It is not possible to use both the Security Defaults and Conditional Access at the same time.

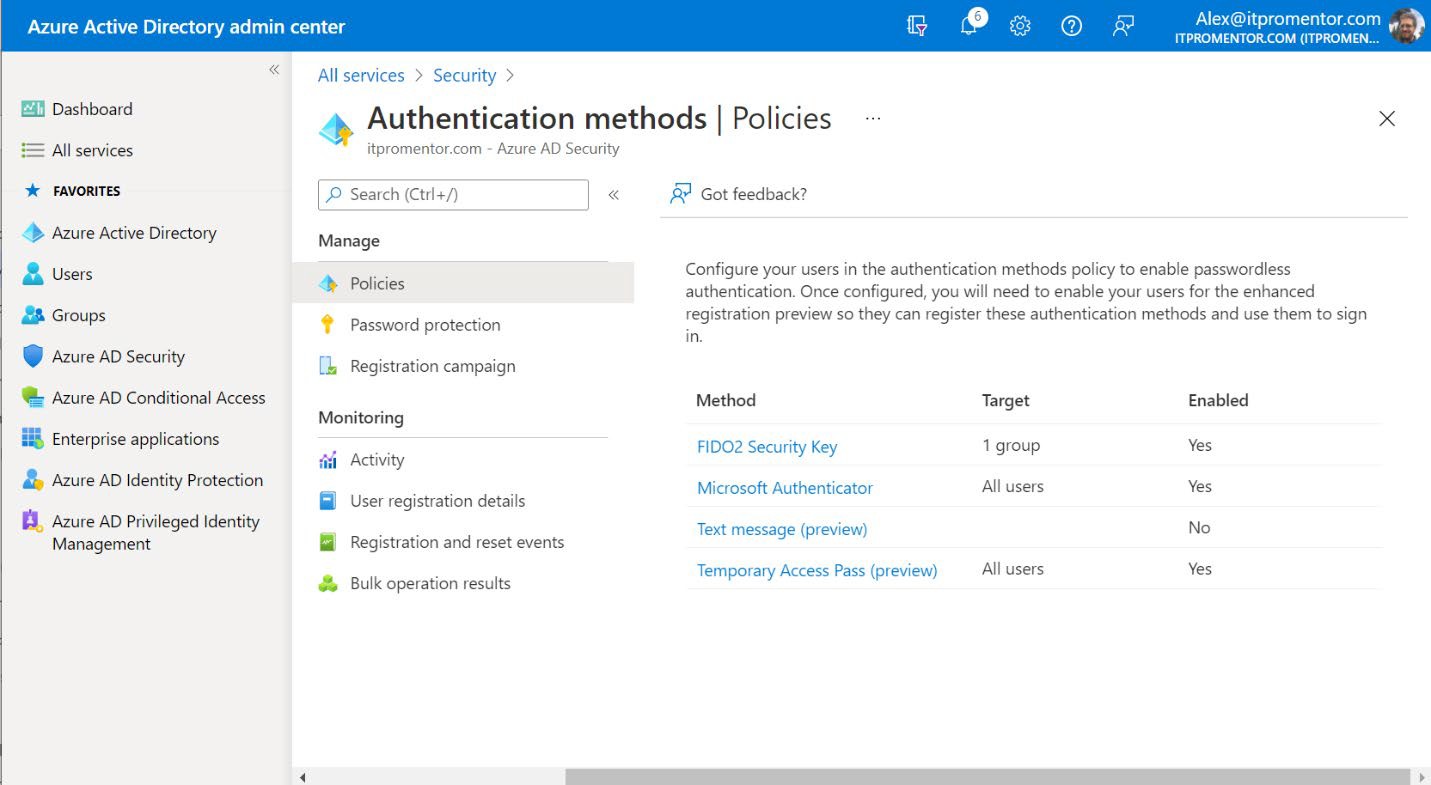
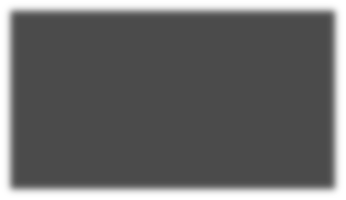
Azure AD > Security > Conditional Access > Policies

[**Per-User MFA**](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates)

Multi-factor Authentication is enabled on the account itself. With Conditional Access available in your subscription, Per-User MFA is not recommended.

Azure AD > Users >

Multi-factor authentication



Next, you can configure your authentication methods. From Azure AD admin center, visit

**Security > Authentication settings > Policies**.

You can read more about the following methods at the links below:

[FIDO2 Security Key](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key) (i.e. hardware tokens) [Microsoft Authenticator](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app)

[Text message](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-sms-signin) (sign-in using your phone number & SMS, e.g. for frontline workers)

[Temporary Access Pass](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-temporary-access-pass) (more on this later)

•

•

•

•

recommend configuring the **Microsoft Authenticator** option for **All users**.

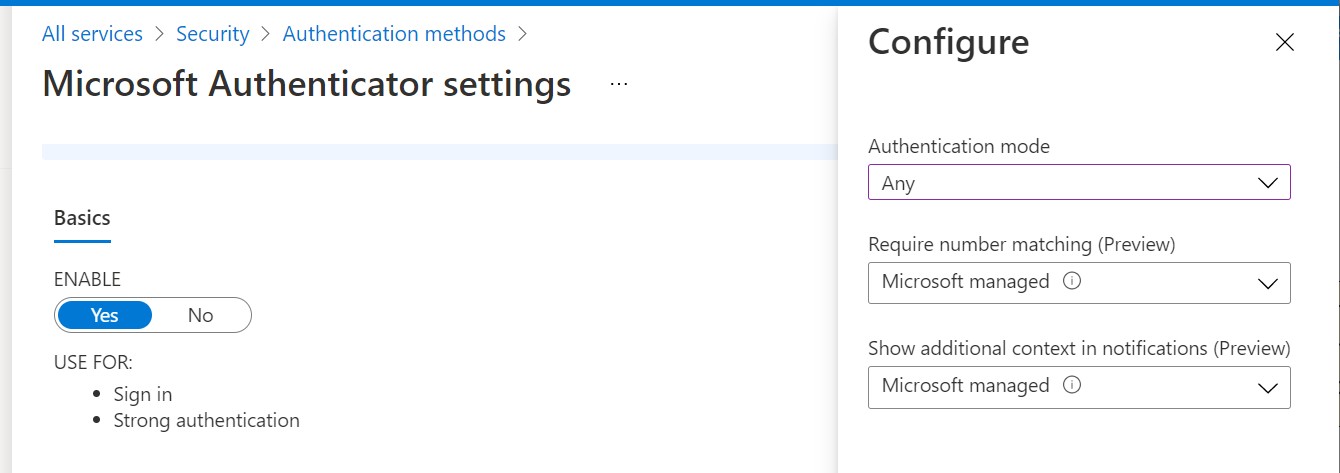
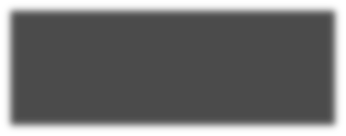
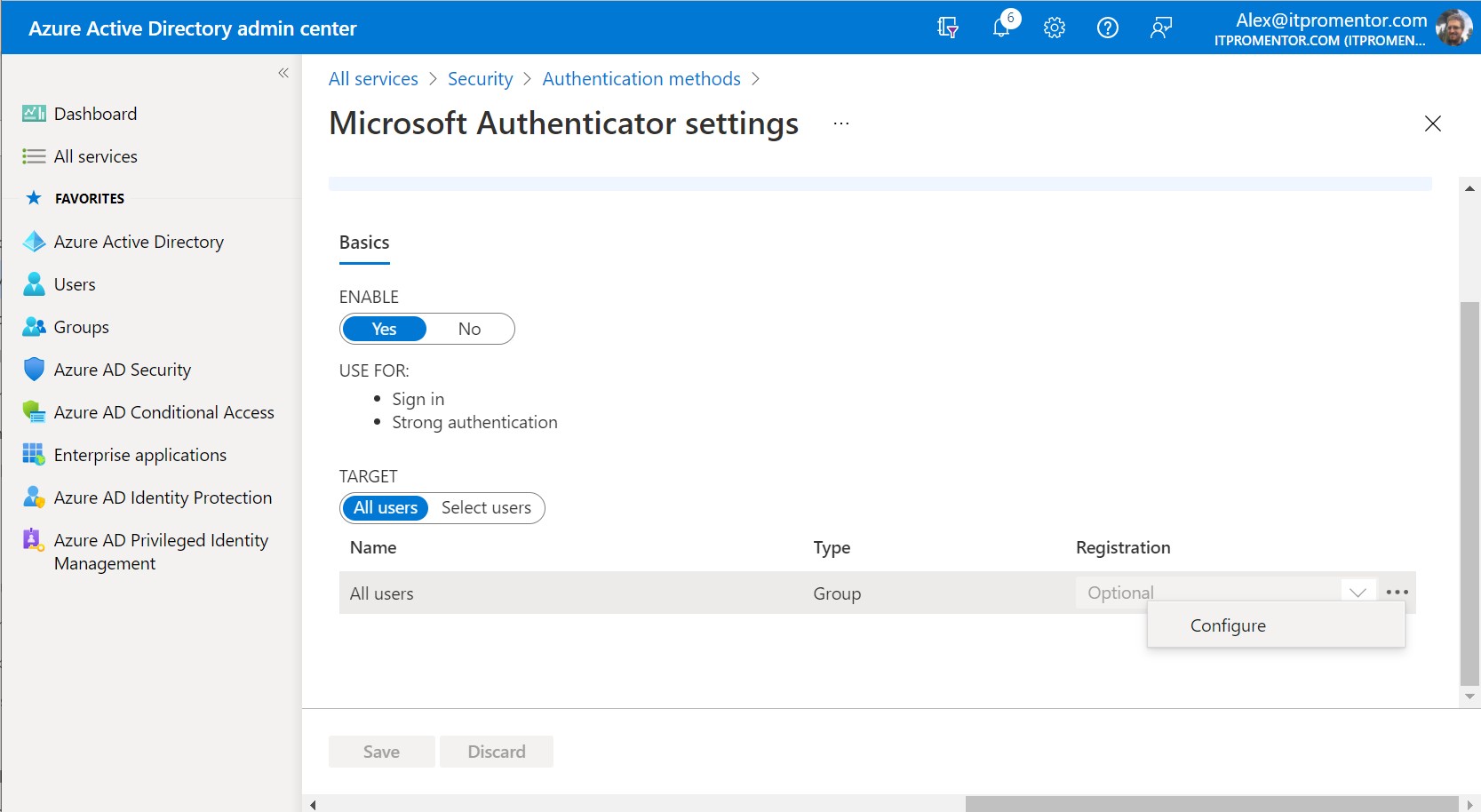
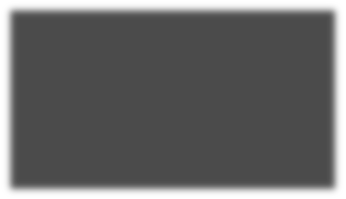
Optionally, you can adjust the settings here to go [passwordless,](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone) meaning the end user will not be prompted for a password but rather, they will only use the Microsoft Authenticator app to sign in. The way this works is by displaying a number on the screen, and the end user will have

to enter that number in their authenticator app.

© Copyright 2019-2022, Azure AD

AZURE AD

7



You can toggle the **Authentication mode** to **Passwordless** if you choose to go that route.

Another way you can improve the Multi-factor experience is by turning on two additional features, called “[Number matching](https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match)” and “[Additional context.](https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context)” believe these will be enabled by default someday in the future, but if you want to opt into those experiences now, switch each option from **Microsoft managed** to **Enabled**.

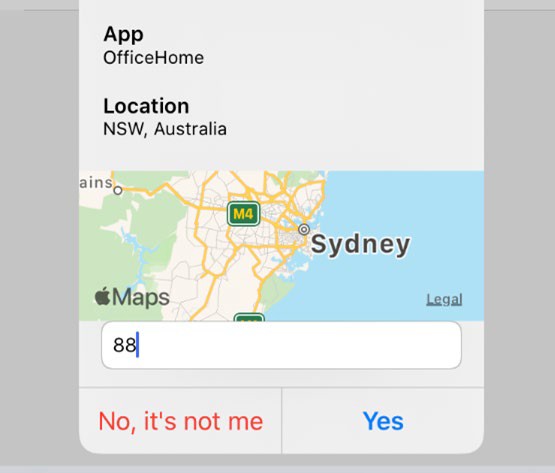
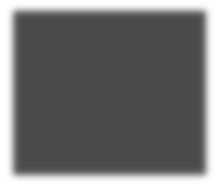
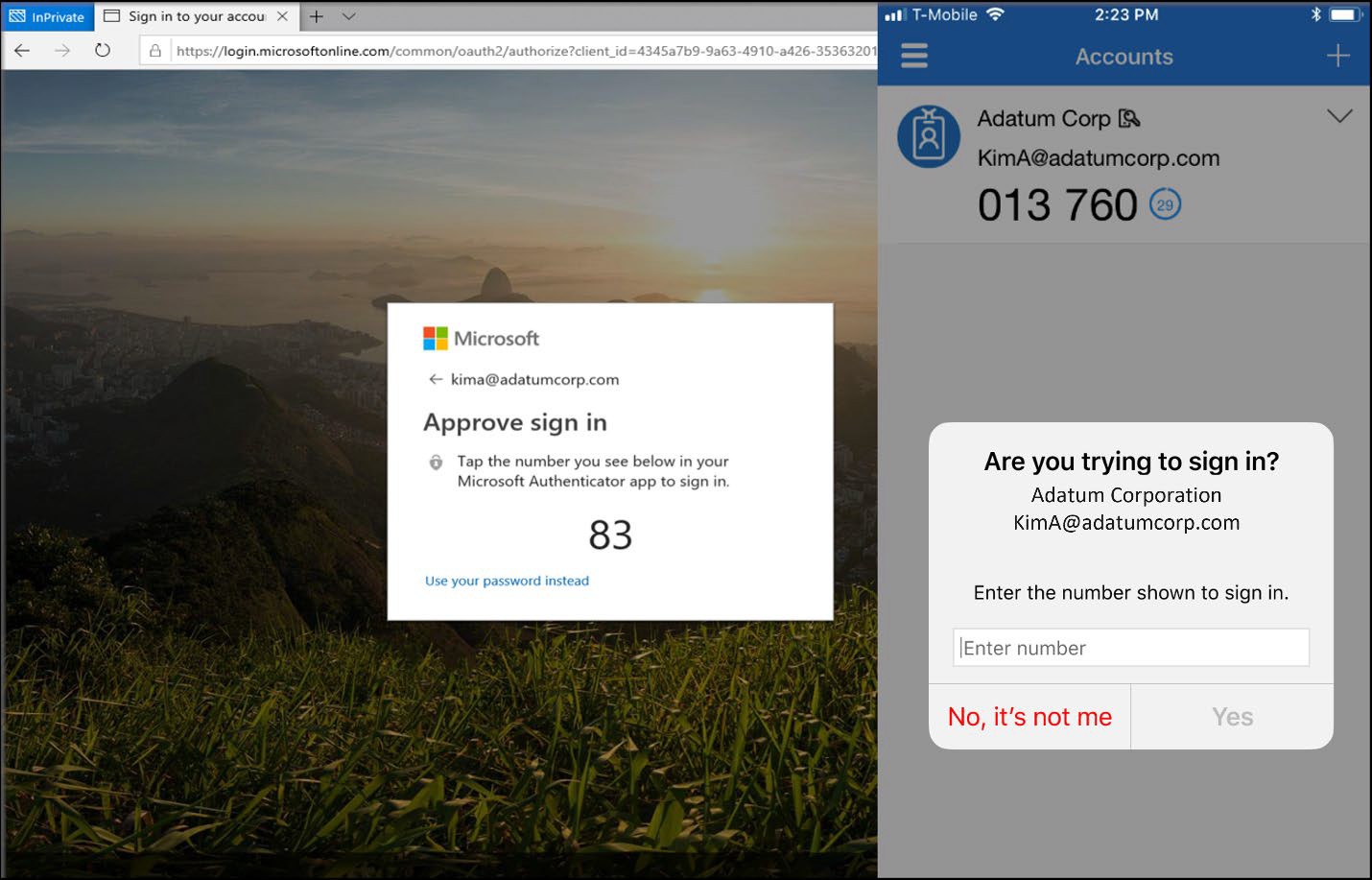
The **number matching** experience is similar to how passwordless works by default (but you can enable this feature without moving to passwordless as well).

© Copyright 2019-2022, Azure AD

AZURE AD

8

Look for the **ellipses** and click **Configure** to toggle other options such as passwordless



**Additional context** goes a step further and it will also display the geolocation to the user so they can see where the authentication is coming from.

However, please note that sometimes this can appear misleading, especially when connecting to public wi-for cellular networks where connections may be routed through a more distant location. personally just like to use number matching without the additional

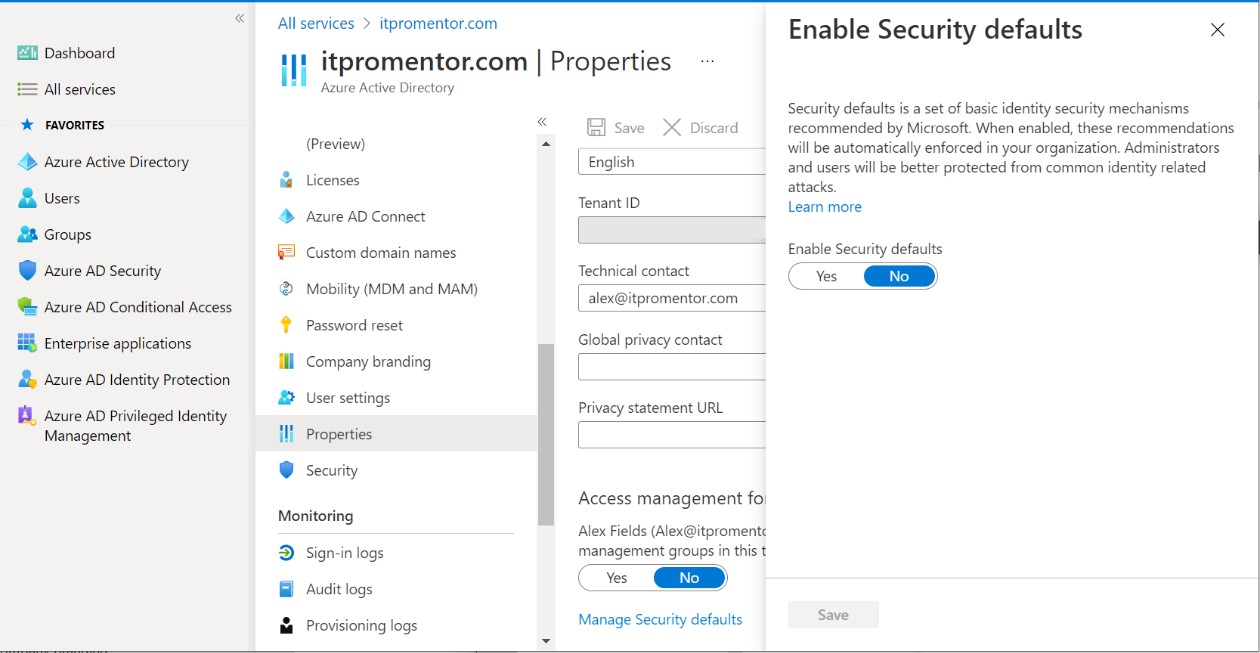
context, but to each their own.

© Copyright 2019-2022, Azure AD

AZURE AD

9

Number matching looks similar to this; the end user must match the number displayed with their app



When you do turn MFA on for users, it is recommended to provide them with some instructional links in advance of this change, so they know what to expect. For example:

* <https://docs.microsoft.com/en-us/azure/active-directory/user-help/>
* <https://www.youtube.com/watch?v=k0oiKQK3LjQ>

They should be prompted to setup MFA authentication mechanisms upon next login, but it is also possible to visit the appropriate setup page manually with this link:

•

<https://aka.ms/mfasetup>

If you previously had MFA configured using per-user MFA with a weaker authentication method

such as SMS text, and you wish to upgrade to Conditional Access and the Authenticator app, do the following:

1.

2.

3.

Run [the script from this page](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#convert-users-from-per-user-mfa-to-conditional-access-based-mfa) before switching from per-user MFA to Conditional Access Enable your CA policies to replace the per-user setting

Consider running an [Authenticator registration campaign](https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-registration-campaign)

* Set up Conditional access according to Best Practices

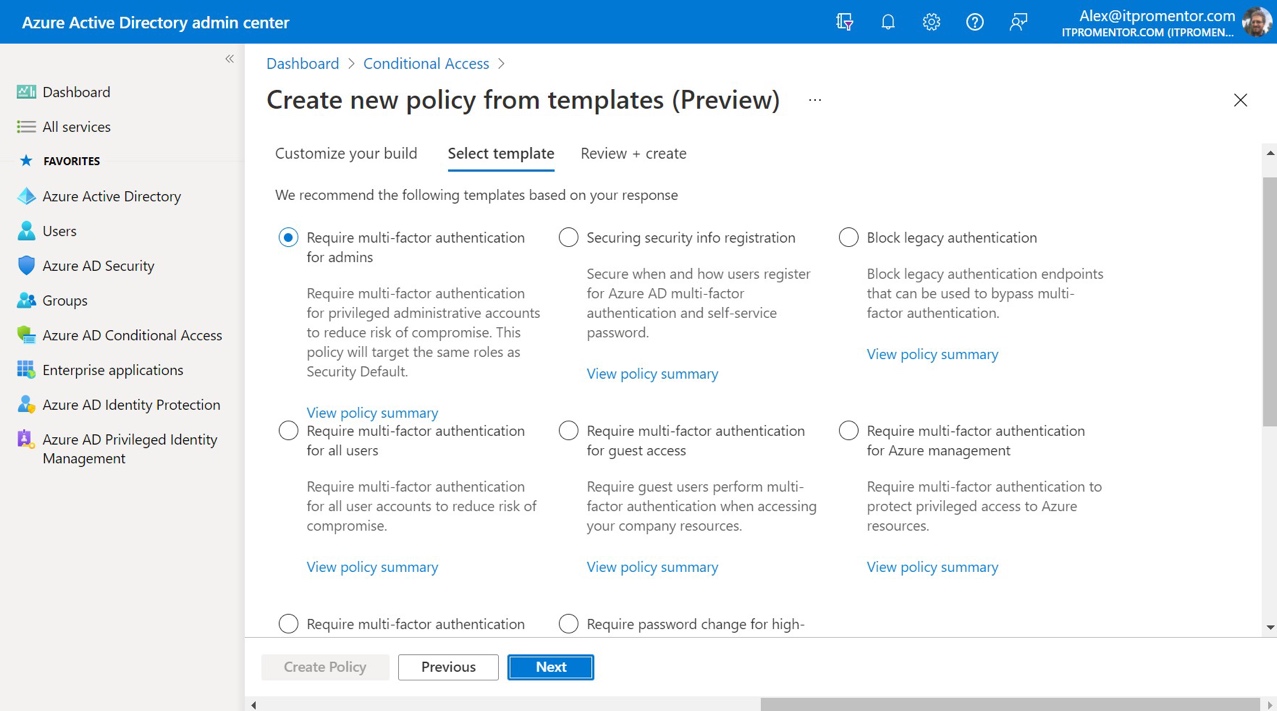
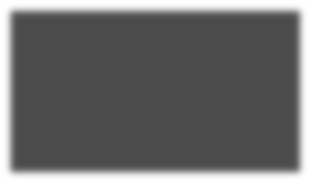
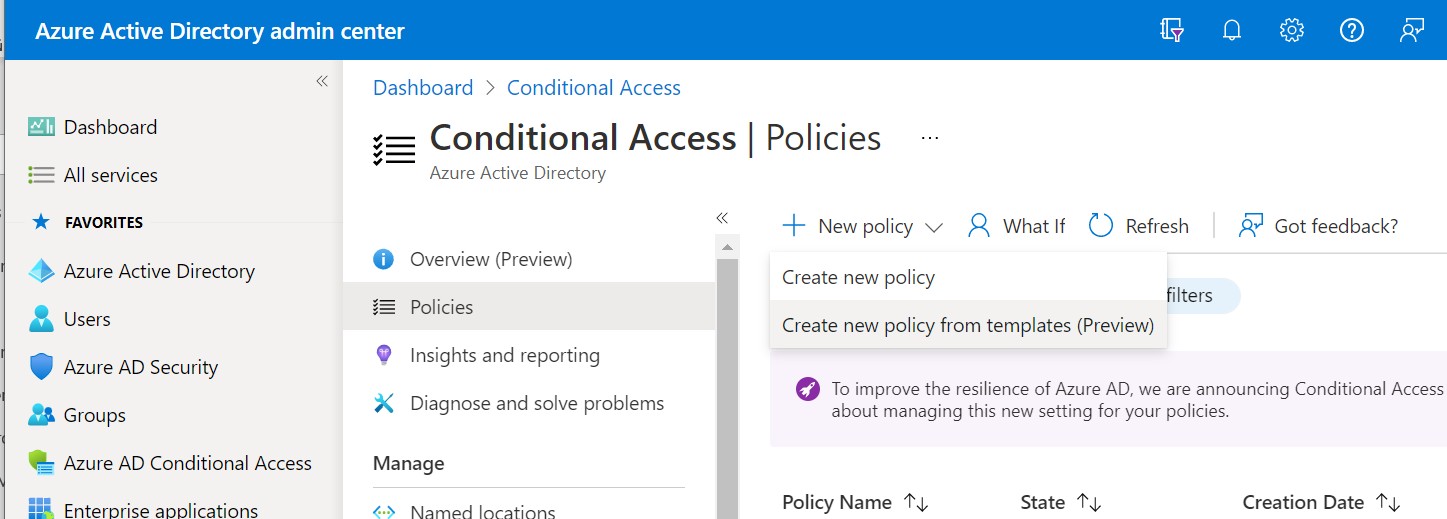
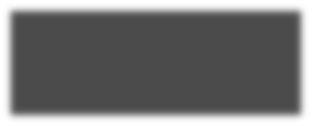
Microsoft enforces a feature known as [Security Defaults,](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-security-defaults) which disables legacy authentication

and enables multi-factor authentication. If the defaults are enabled in your tenant, be sure to disable them before configuring custom Conditional access policies. You cannot mix them.

© Copyright 2019-2022, Azure AD

AZURE AD

10



Microsoft provides several [policy templates](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common#conditional-access-templates-preview) that you can use as a starting point (using the

**Create new policy from templates option**).

Start with the **Identities** template category.

Be sure to configure at least these authentication policies to replace the Security Defaults:

[**Block legacy authentication**](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-block-legacy)[**Require MFA for Admins**](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa)

[**Require MFA for Azure management**](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management)

[**Require MFA for All users**](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa)

•

•

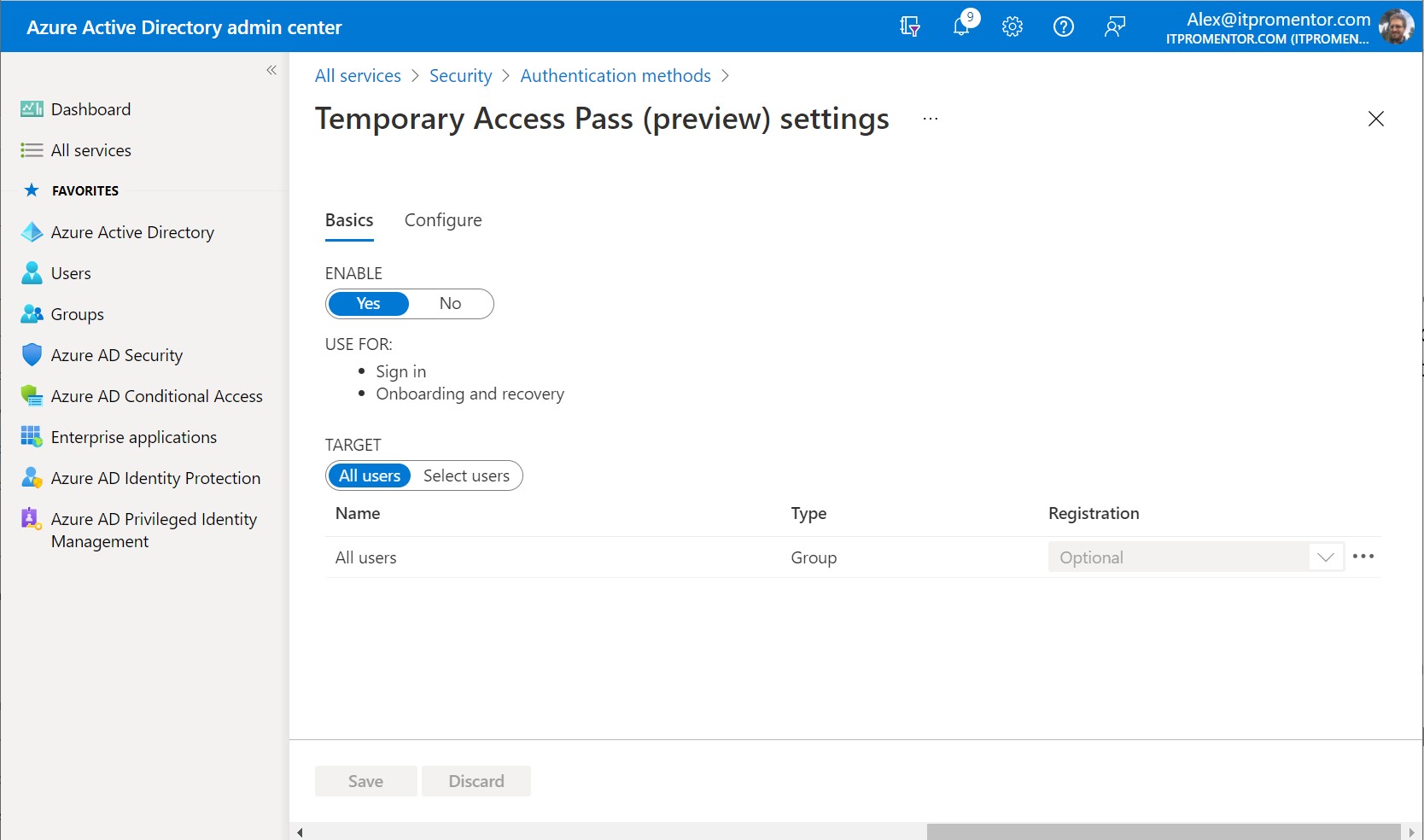
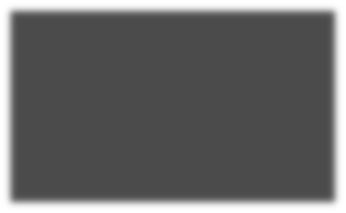
•

•

© Copyright 2019-2022, Azure AD

AZURE AD

11



You should also review the [Best Practices for Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access#follow-best-practices) published by Microsoft. For additional guidance “from the field,” refer to my **Conditional Access Best Practices and Policy Examples** guide.

* Enable Temporary Access Pass (TAP)

TAP is an authentication method that can be used to help end users out of a jam. For example, if they lose a primary authentication method, or if they need to setup a new method and do not have their old one. Another common use case is to secure the initial MFA registration using a TAP. With TAP enabled, an admin can issue a temporary passcode. Find this option in Azure AD

admin center **Security > Authentication settings > Policies**.

Open the **Temporary Access Pass** page to enable the feature. Also see the **Configure** tab for additional options (like maximum lifetime, etc.). If you deployed [this Conditional access policy](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-registration) to secure the MFA registration process (also available from the templates), then a TAP can be one of the auth methods. See [this article](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-temporary-access-pass#create-a-temporary-access-pass) for more details on creating and using a TAP.

* Configure device settings for Azure AD joined devices

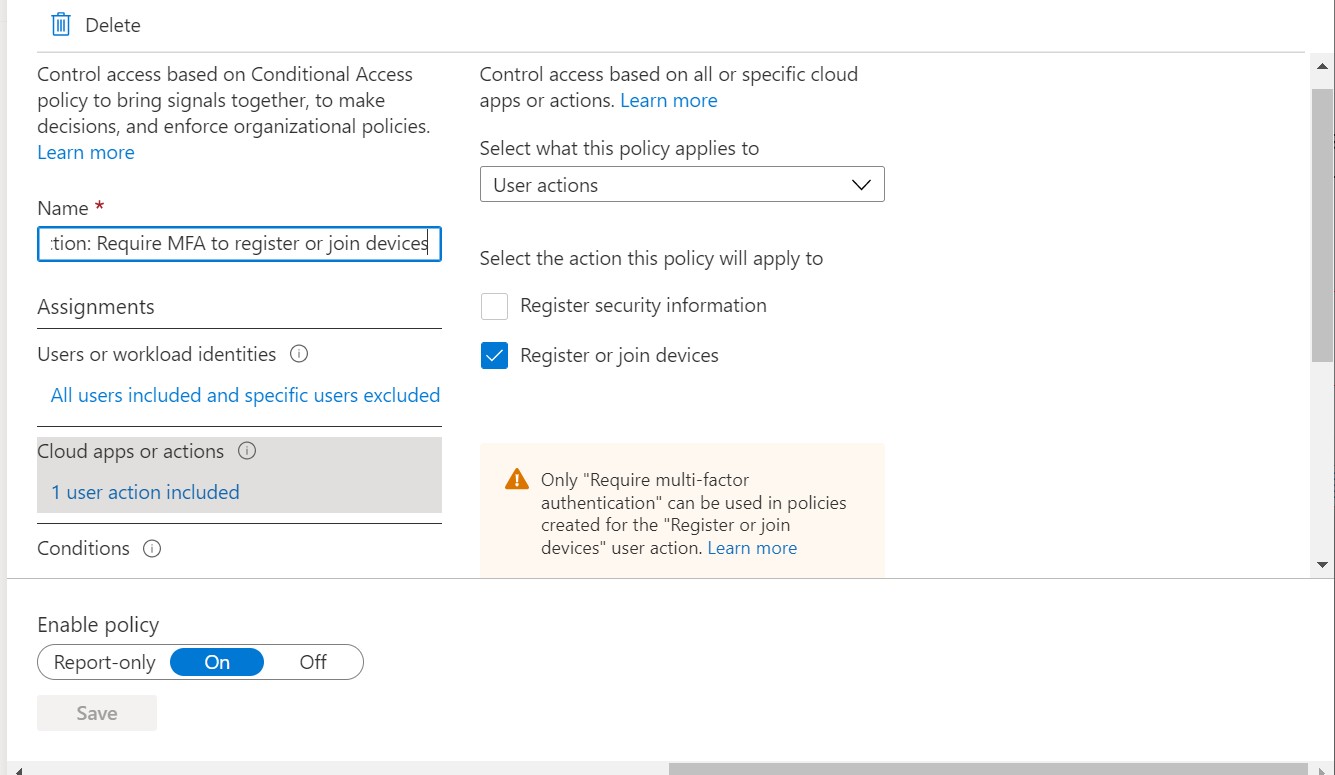
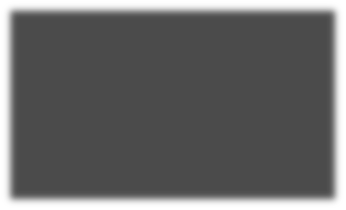
The setting to require MFA for device registration and join operations is now available as a

Conditional Access policy. Do not enable this policy until you have already onboarded your users for Multi-factor Authentication.

© Copyright 2019-2022, Azure AD

AZURE AD

12



*Note: Users may be prompted to register for MFA if they have not already.*

Under **Azure AD > Devices > Device settings**, you can find more options for configuring Azure AD Join, for example you can constrain who is allowed to join devices (we will look at this option

in more detail later when we constrain it to our *licensed* users).

© Copyright 2019-2022, Azure AD

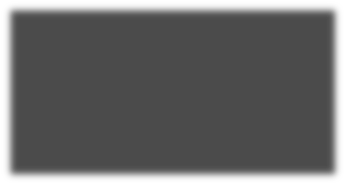
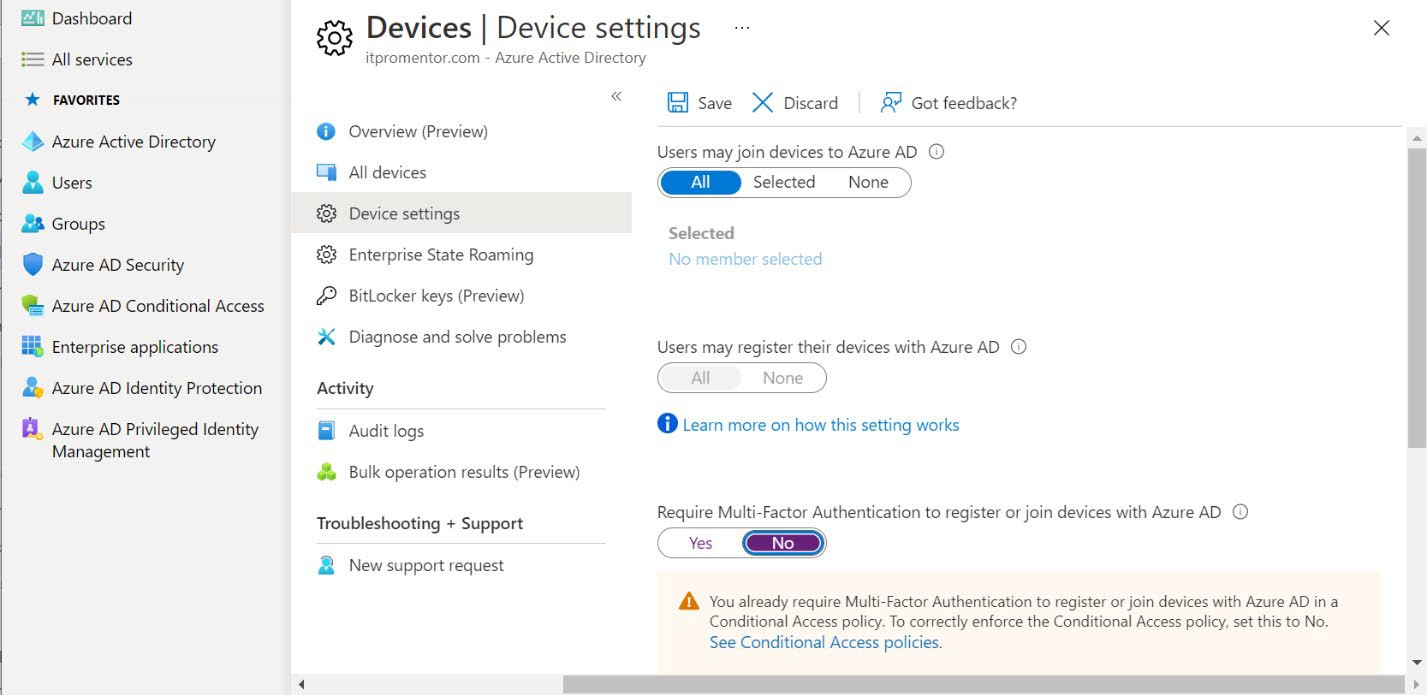
AZURE AD

13

Pick **Register or join devices**, and then enable Multi-factor under **Access controls > Grant**

Choose **User actions**

instead of Cloud apps



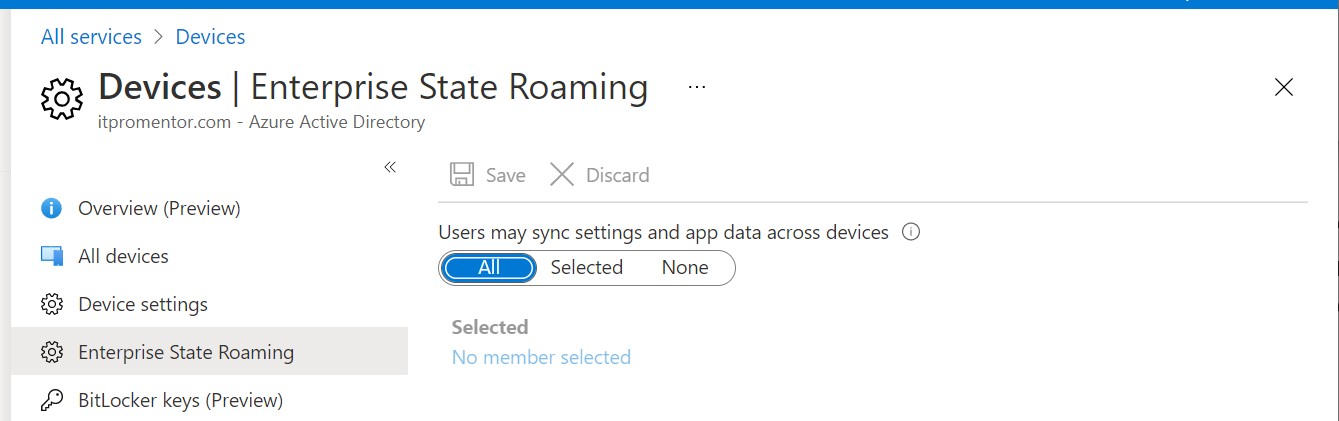
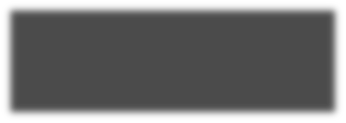
Otherwise, if you deployed the Conditional Access policy to require MFA for device registration or Azure AD join, you will want to disable the same option below.

Scrolling down further on this page you will find two more links worth mentioning.

© Copyright 2019-2022, Azure AD

AZURE AD

14



The first, **Manage Additional local administrators…** will simply link you over to the Azure AD role called **Device administrators**. By default, this role is given local admin on all Azure AD joined devices, as well as all Global admins plus the account that performs the initial Azure AD Join operation. This is **not** a role use in the SMB space typically.

The second link brings you over to the **Enterprise State Roaming** settings page, and do recommend enabling this, so that user settings & preferences can be synced between devices.

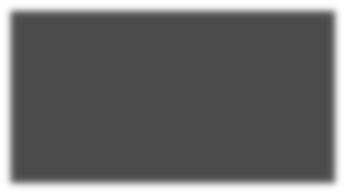
* Configure the password expiration policy

If you are syncing your identities using Azure AD Connect, then the password expiration policy will follow what you have configured on-premises. For cloud-native accounts, visit the Microsoft 365 admin center ([https://admin.microsoft.com](https://admin.microsoft.com/)) and navigate to **Settings > Security & Privacy**.

© Copyright 2019-2022, Azure AD

AZURE AD

15



Click **Password expiration policy**. Microsoft’s latest password guidance suggests that you set the passwords to **Never** expire (just clear the selection to ensure there is no expiry).

Only do this if:

1.

2.

3.

4.

You are not subject to legal or compliance requirements that suggest the opposite Multi-factor authentication is already enforced org-wide

You are alerted when a possible credential leak has occurred

You are for suspicious activities which indicate certain accounts may be compromised

Otherwise, you will probably want to rotate the password at least annually or in accordance with other compliance and regulatory requirements that you might have.

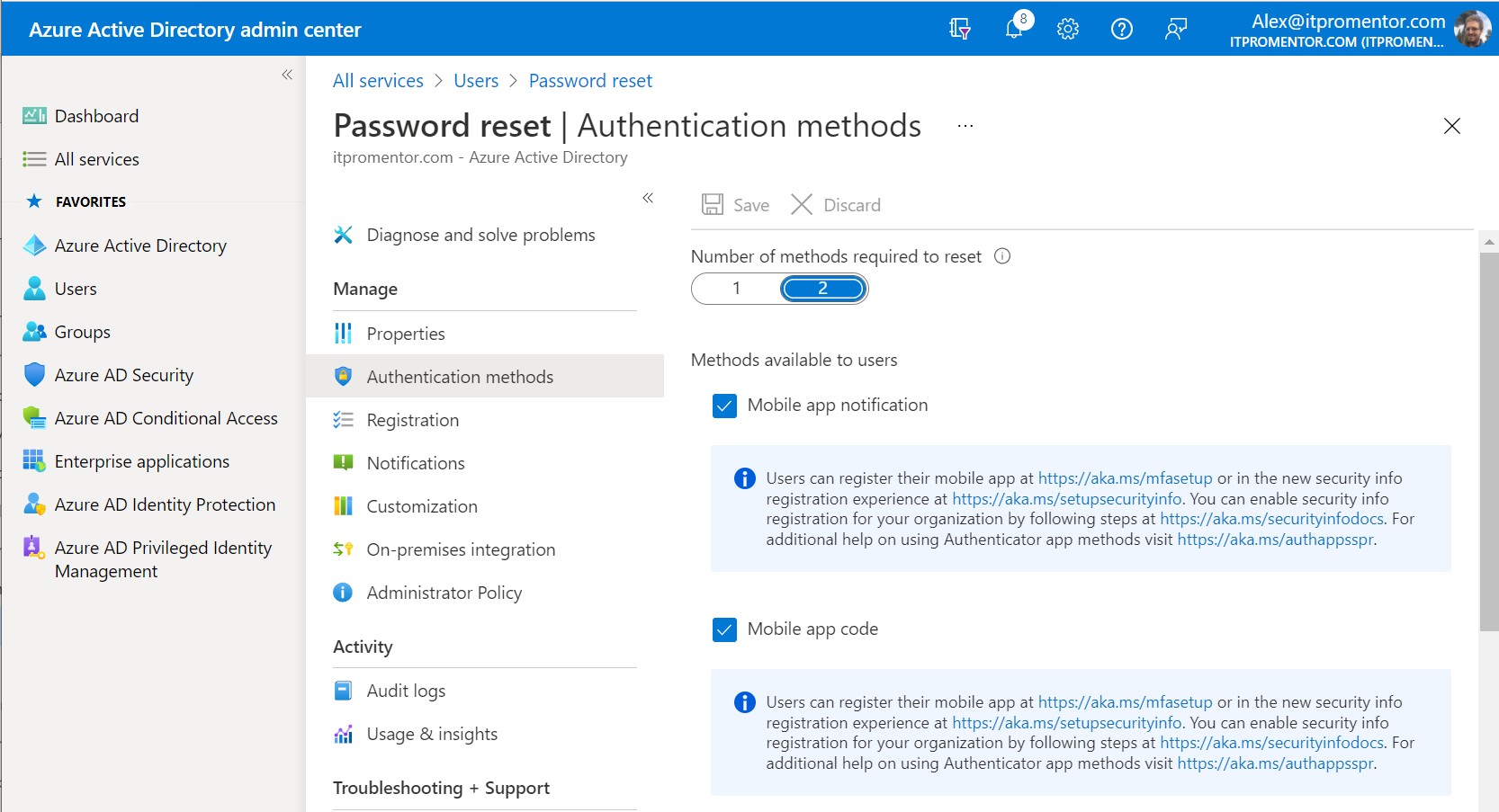
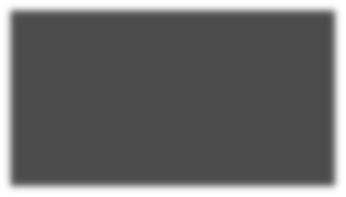
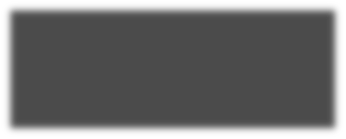
If you are successfully leveraging all the other critical identity protections such as MFA, password protection, Conditional access and so forth, across the *entire* organization AND you feel confident that you would be able to detect and respond to an identity breach, only at that point

should you move to non-expiring passwords. Otherwise, stick to expiry.

© Copyright 2019-2022, Azure AD

AZURE AD

16



Items of Recommended Importance

* Enable Self-service password reset (SSPR)

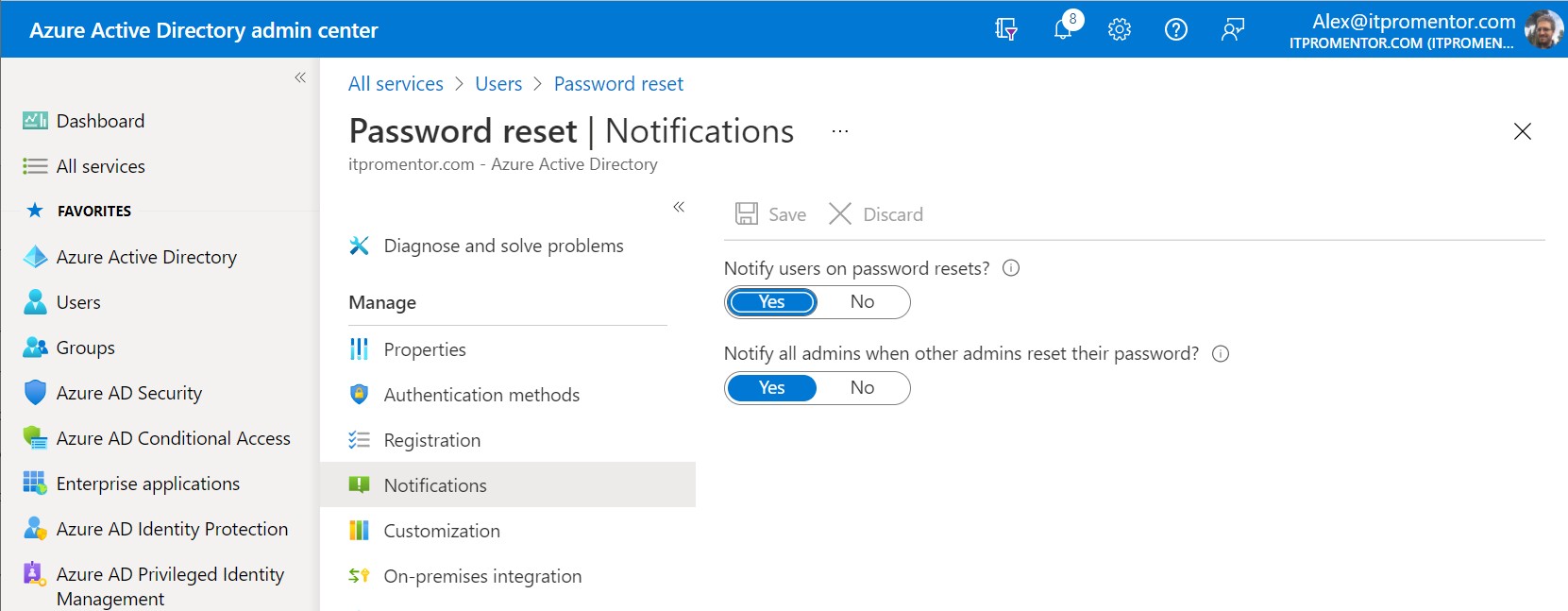
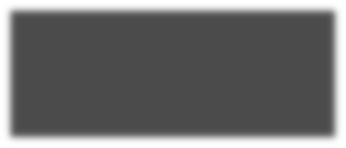
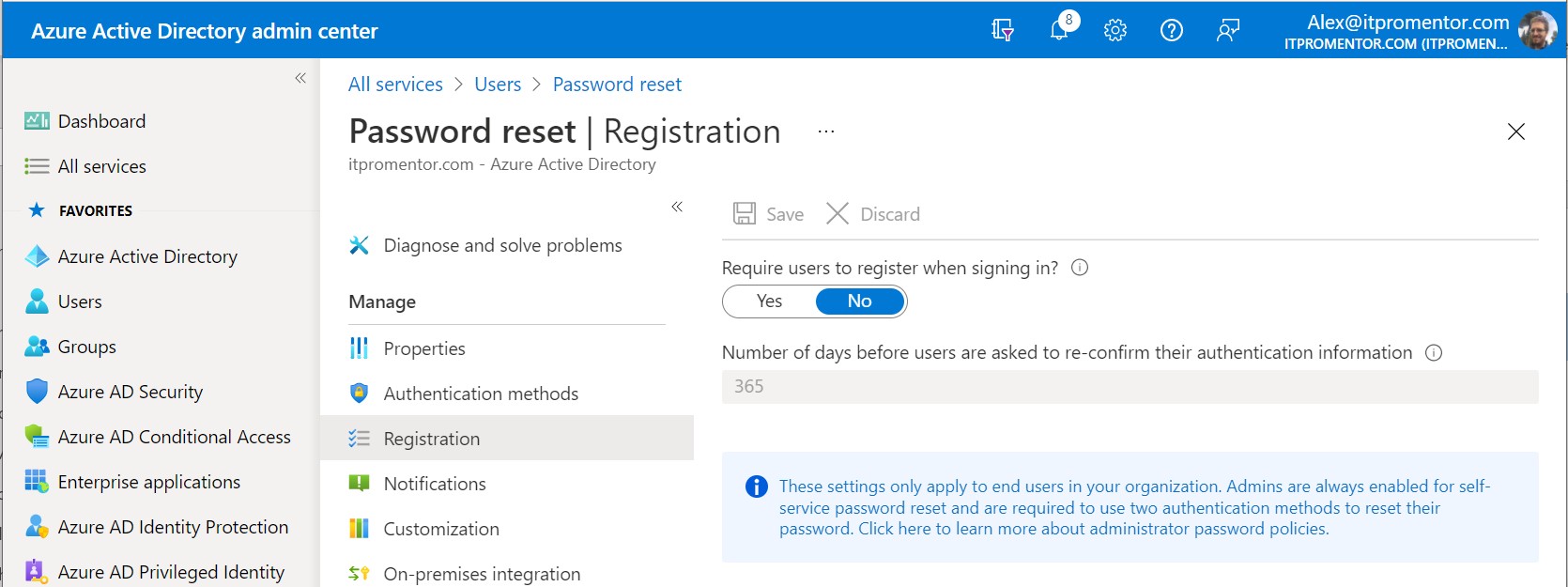
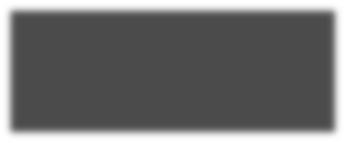
Navigate to **Users > Password reset**. Under **Properties**, Pick **All** to enable SSPR for all users.

***Authentication methods***: require **2** methods and select at least *Mobile app notification*, *Mobile app code*, and others such as *Mobile phone* and *Email* as you prefer. *P.S.: do not recommend the ‘Security questions’ option.*

© Copyright 2019-2022, Azure AD

AZURE AD

17



***Registration:*** With combined registration enabled, users should already be prompted to register their security information, so this is moot. However, you can set this option to **Yes** if you want to enforce re-registration regularly so that users are asked to re-confirm on a specified interval. normally just select **No** here. But to each their own.

***Notifications***: Pick **Yes** for both user and admin notifications

*Note: if you also have Azure AD Connect in place for on-premises AD, you must also enable password write-back from the* ***On-premises integration*** *node in*

*the left navigation.*

© Copyright 2019-2022, Azure AD

AZURE AD

18

* Follow best practices for security groups

Security groups in Azure AD can be either static or dynamic, and they can contain either devices *or* users. However, a security group should not contain *both* user *and* device objects (pick one or the other for each group you create).

*Note: This is unlike Microsoft 365 groups, which can only contain users.*

When you name security groups, consider using a naming convention so that you can quickly tell that this is a security group, and not a Microsoft 365 Group, and what the group is “for.”

Examples:

**SGU-Marketing**: Members of the Marketing department

**SGU-License-Frontline**: Users who have the ‘Frontline worker’ licensing assignment **SGU-Exclude-Baseline**: Members of this group are excluded from the security baseline **SGD-BYOD-Android**: Personally owned Android devices

**SGD- CORP-Windows**: Company-owned Windows devices

•

•

•

•

•

In these examples, the **SGU** prefix denotes groups of *users*, whereas **SGD** denotes groups containing *devices*. Avoid *nesting* security groups within each other whenever possible. Aim for a “flat” management structure with your groups. Security group nesting currently has very limited support in Azure AD. See [this Microsoft Docs article](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal) for more details.

As well, you should always avoid assigning resources directly to end users. Security groups can help you to organize and scale your management.

* Users  Groups  Licenses
* Users  Groups  Applications
* Users  Groups  Policies

For example, you should plan to assign your Microsoft 365 product licenses using a security group. Let us assume that you have two basic user profiles. "Standard Users" and "Mobile Users." A *Standard* user is issued a Windows laptop computer with Microsoft 365 Office applications. Meanwhile, a *Mobile* user is essentially a BYOD user who only uses their phone or a tablet to access Outlook and Teams, and likely nothing else. For this scenario you might create

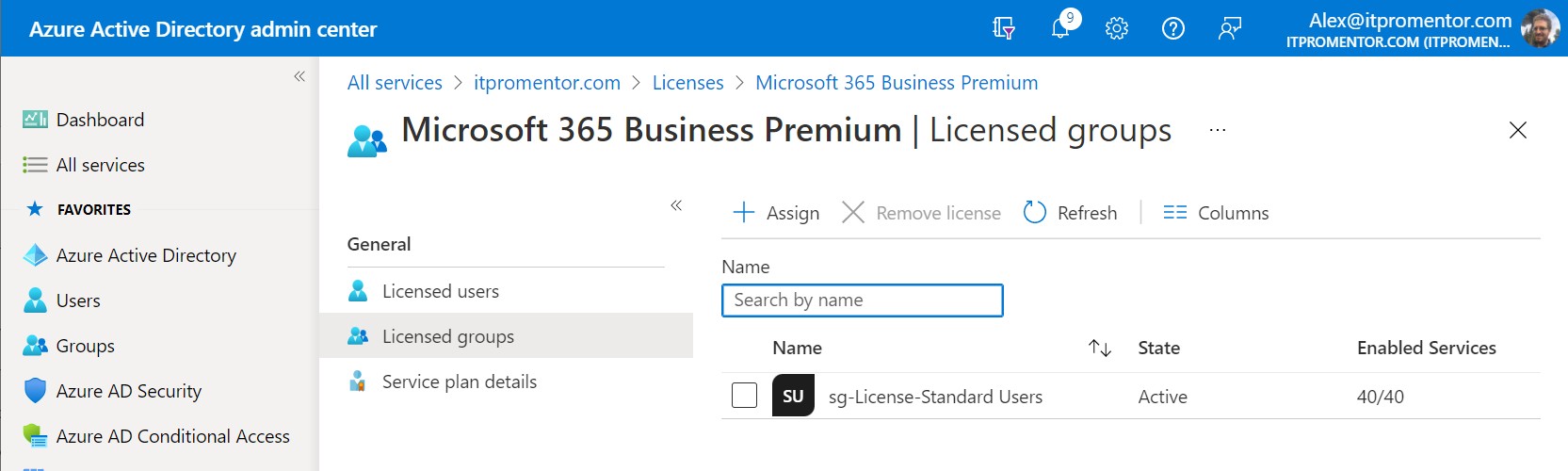
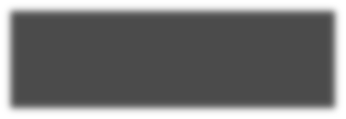
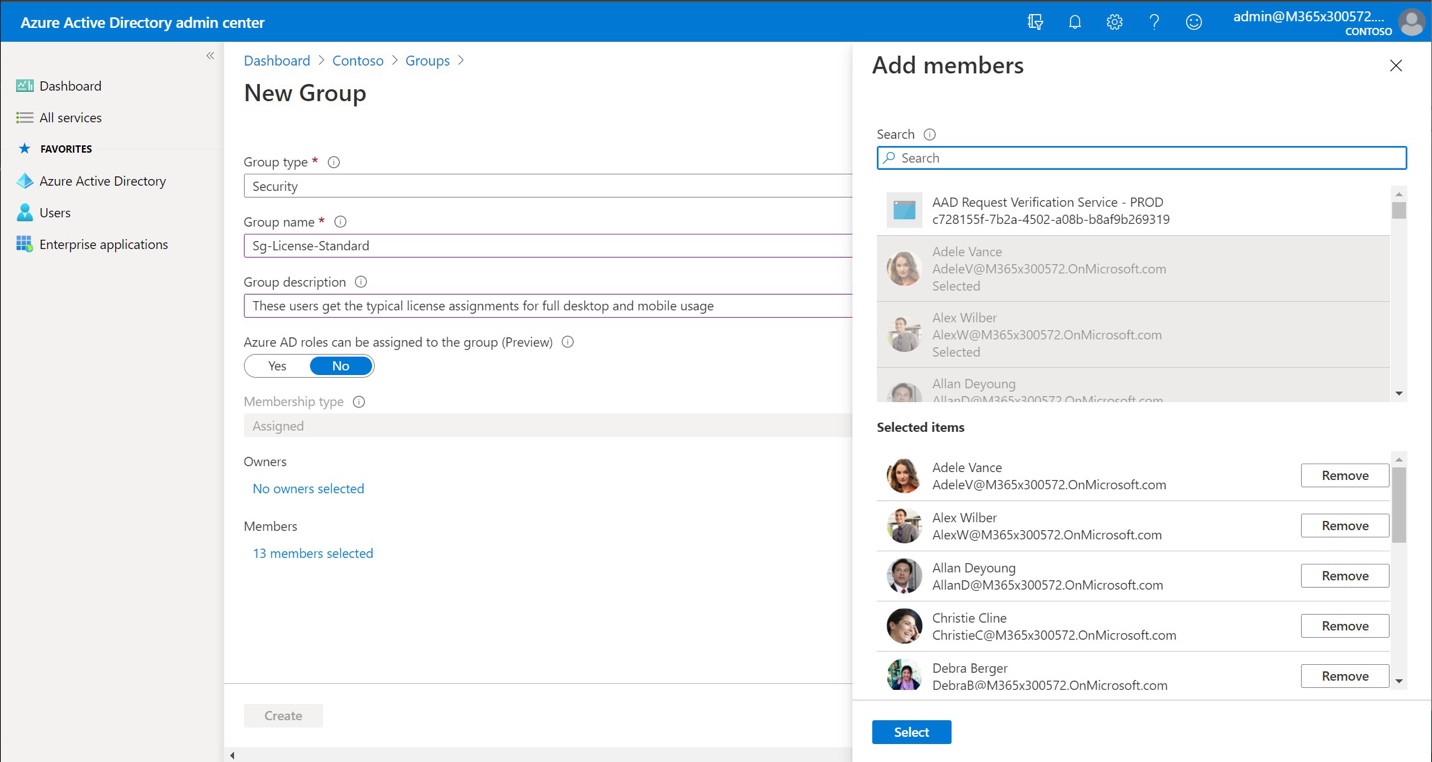
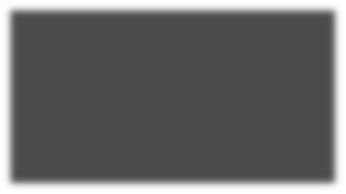
two groups:

* **SGU-License-Standard**
* **SGU-License-Mobile**

© Copyright 2019-2022, Azure AD

AZURE AD

19



Then, you would assign a subscription such as **Microsoft 365 Business Premium** to the *Standard* group, but the *Mobile* group may get a different assignment. Perhaps the **Microsoft 365 F1** plan. This way, you would be able to manage who gets what software using the security

groups that you created.

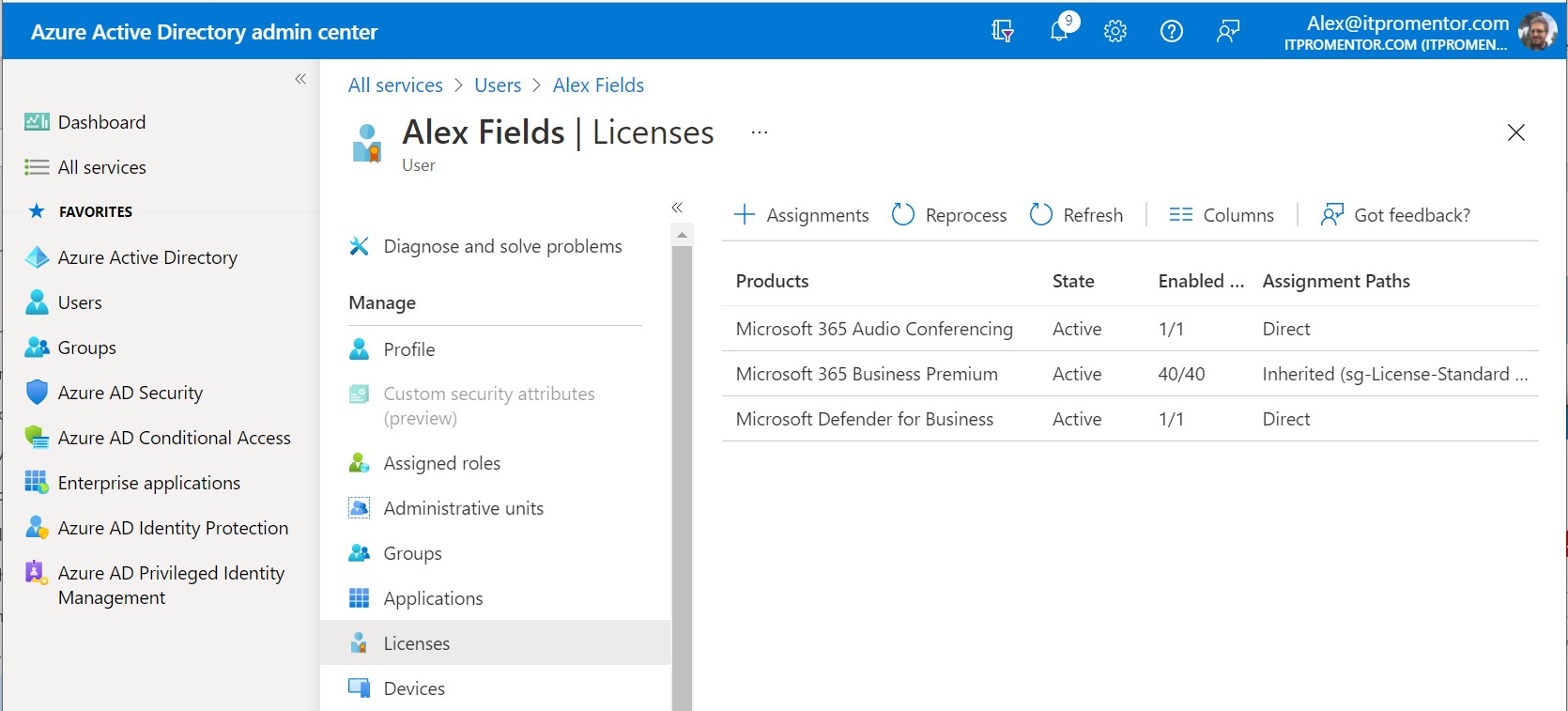
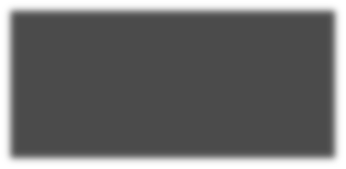
Create your security groups and name them so that they make sense for your use cases. Assign the users to each group that should receive the corresponding licenses. Once your groups are ready, you can navigate to **Azure AD > Licenses > All products**. Now **Select** the license that

should be assigned to standard users, and go to **Licensed groups** to make your assignment.

© Copyright 2019-2022, Azure AD

AZURE AD

20



You can verify it is working by navigating to a user in Azure AD that belongs to this security group. Click **Licenses** to see how they are receiving their license assignments.

In the example above, have some licenses with ***Direct*** assignment, as well as ***Inherited*** via our security group. (And if you want to remove any direct assignments simply click on the license and then click **Remove license**.)

* Restrict Azure AD Join and Auto-enrollment

Once you have established security groups to manage your licenses, then you can also leverage these same security groups to control (1) who can join devices to Azure AD, (2) who can sync their settings with Enterprise State Roaming, and (3) who can auto-enroll their Windows devices with Intune. Only fully licensed Microsoft 365 users (or users with Windows 10 and Enterprise

Mobility + Security) should be allowed access to these features.

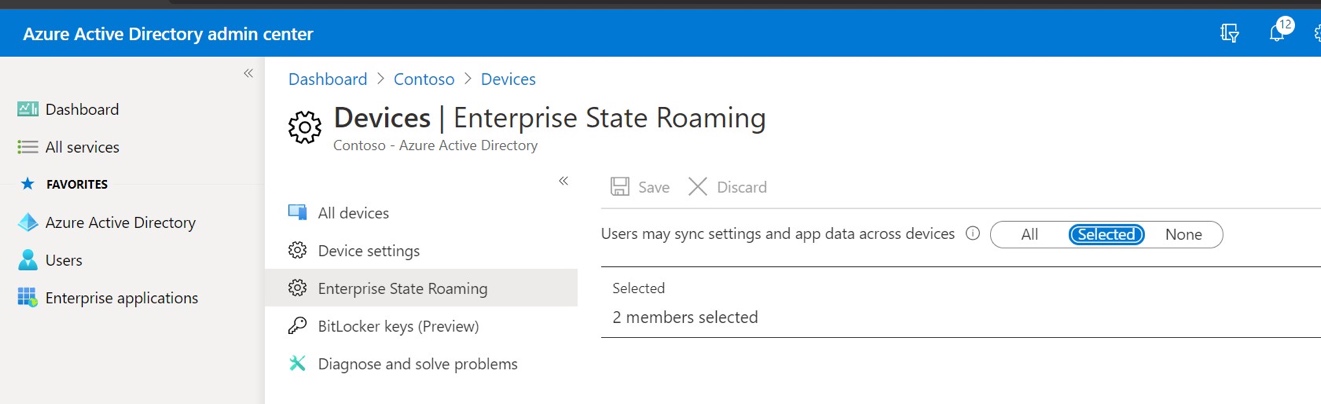
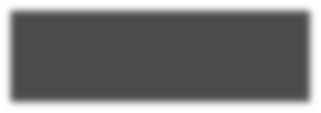
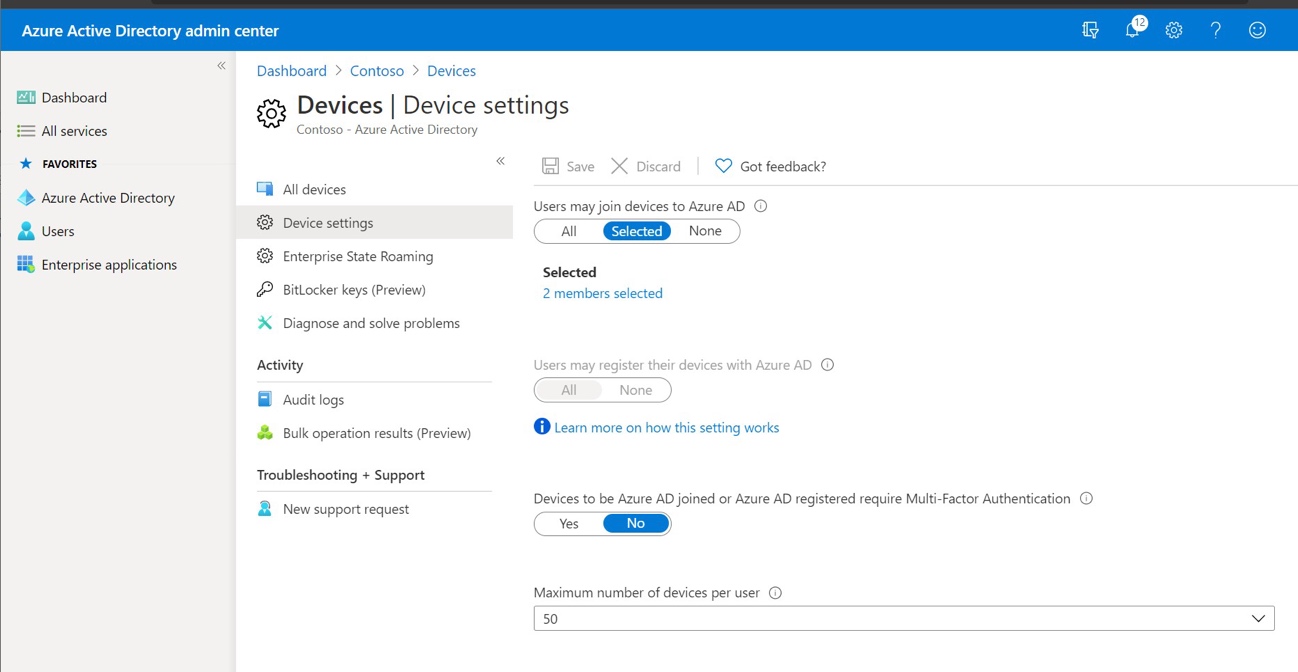
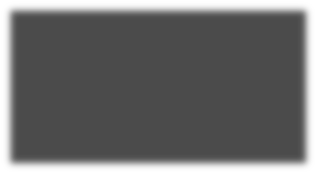
Navigate to **Azure AD > Devices > Device settings**. Find the option **Users may join devices to Azure AD**. Click **Selected**, then click to add members below. Click **Add** and find the security

group(s) for your licensed user accounts. Click **OK**.

© Copyright 2019-2022, Azure AD

AZURE AD

21



**Save** the changes on the **Device settings** screen. This means that only the users specified by the

selected security group(s) will be able to join Windows devices to Azure AD.

Similarly, you can accomplish the same for *Enterprise State Roaming* from **Devices > Enterprise State Roaming** on the left menu. Repeat the above process to add the licensed user groups

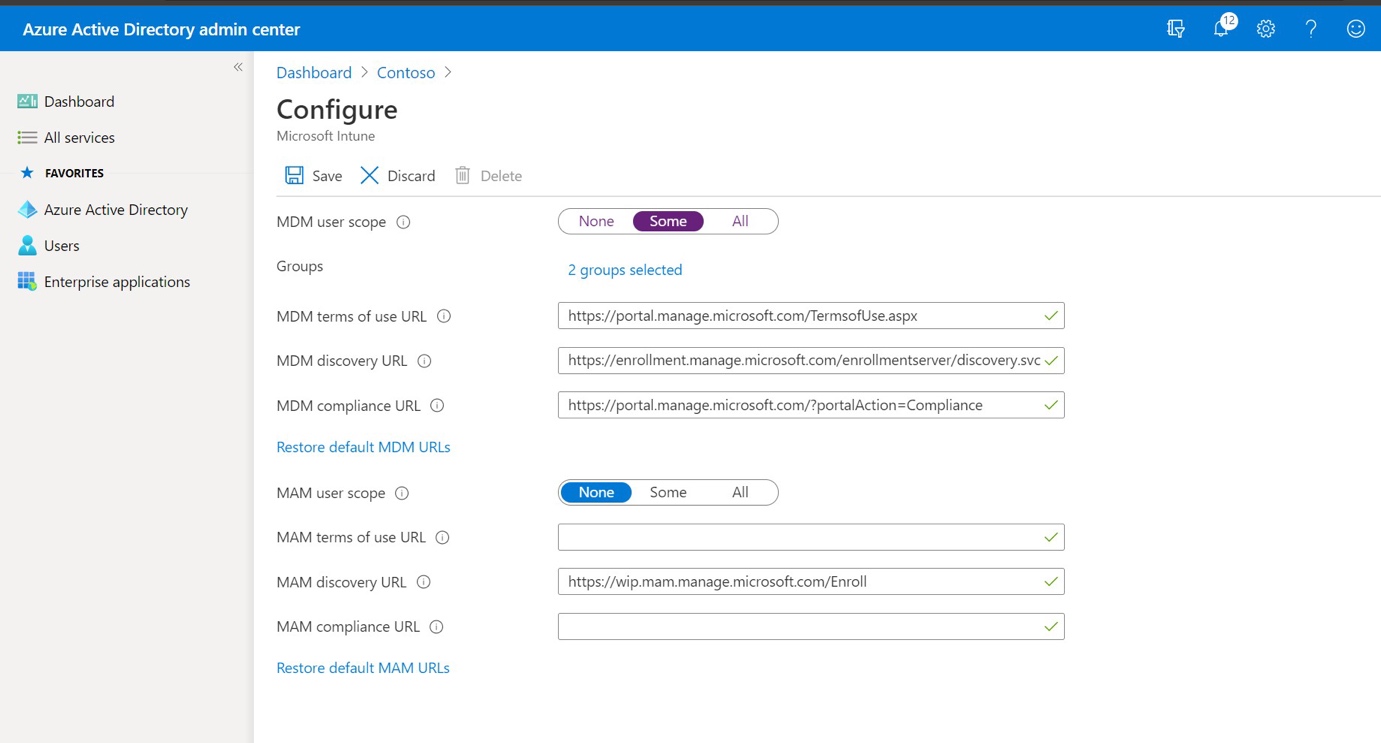
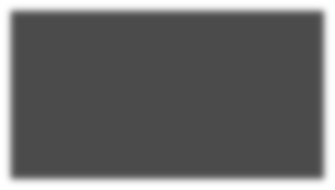
under **Selected** to enable Enterprise State Roaming. **Save** the changes on this screen.

Now navigate to **Azure AD > Mobility (MDM + MAM) > Microsoft Intune**.

© Copyright 2019-2022, Azure AD

AZURE AD

22



Under **MDM User scope** click **Some** and then **Add** the same security group(s) again. This means that only the users specified by the selected security group(s) will be enrolled automatically for MDM via Intune when they register or join devices to Azure AD. You could repeat the same steps under the MAM user scope if you plan to deploy Windows Information Protection for

personally owned devices. Read more about this setting in the Intune Best Practices Guide.

* Restrict user access and app registration in Azure AD

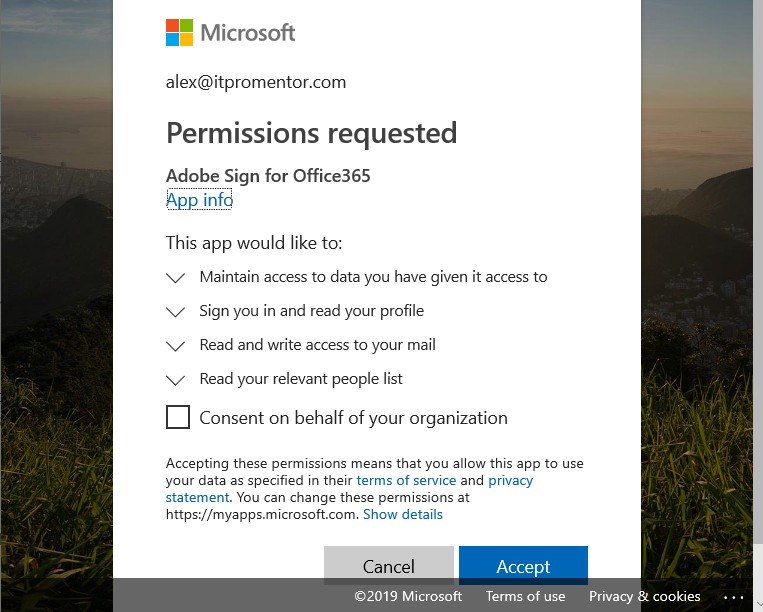
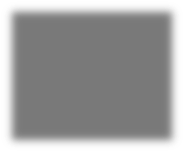
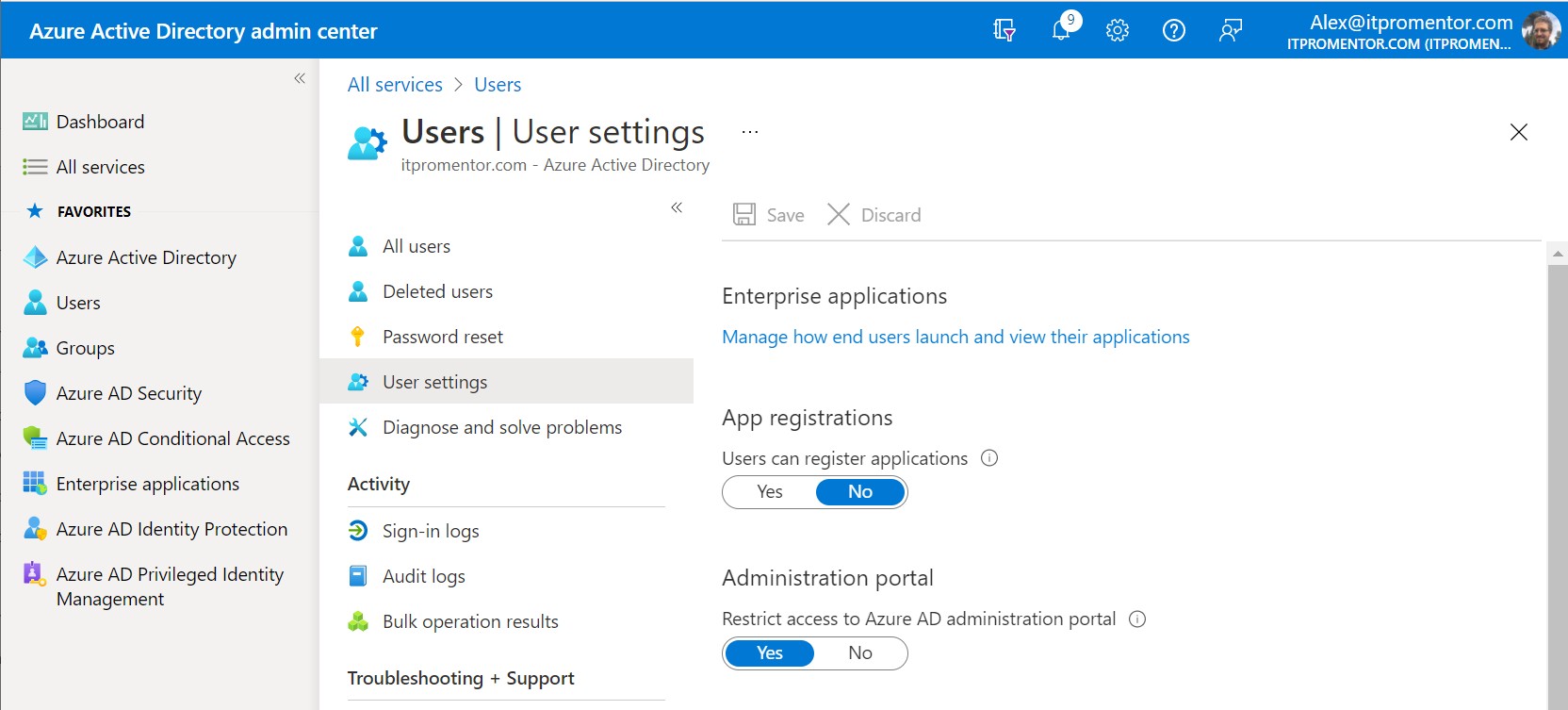
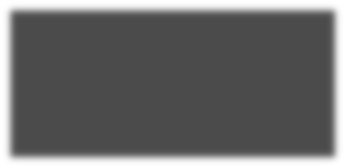
By default, any user can register custom developed applications and access the Azure AD admin portal. If these are not requirements for the general end user in your organization, these can be

disabled. Navigate to **Users > User settings** to find these options.

© Copyright 2019-2022, Azure AD

AZURE AD

23



* Manage application consent and permissions

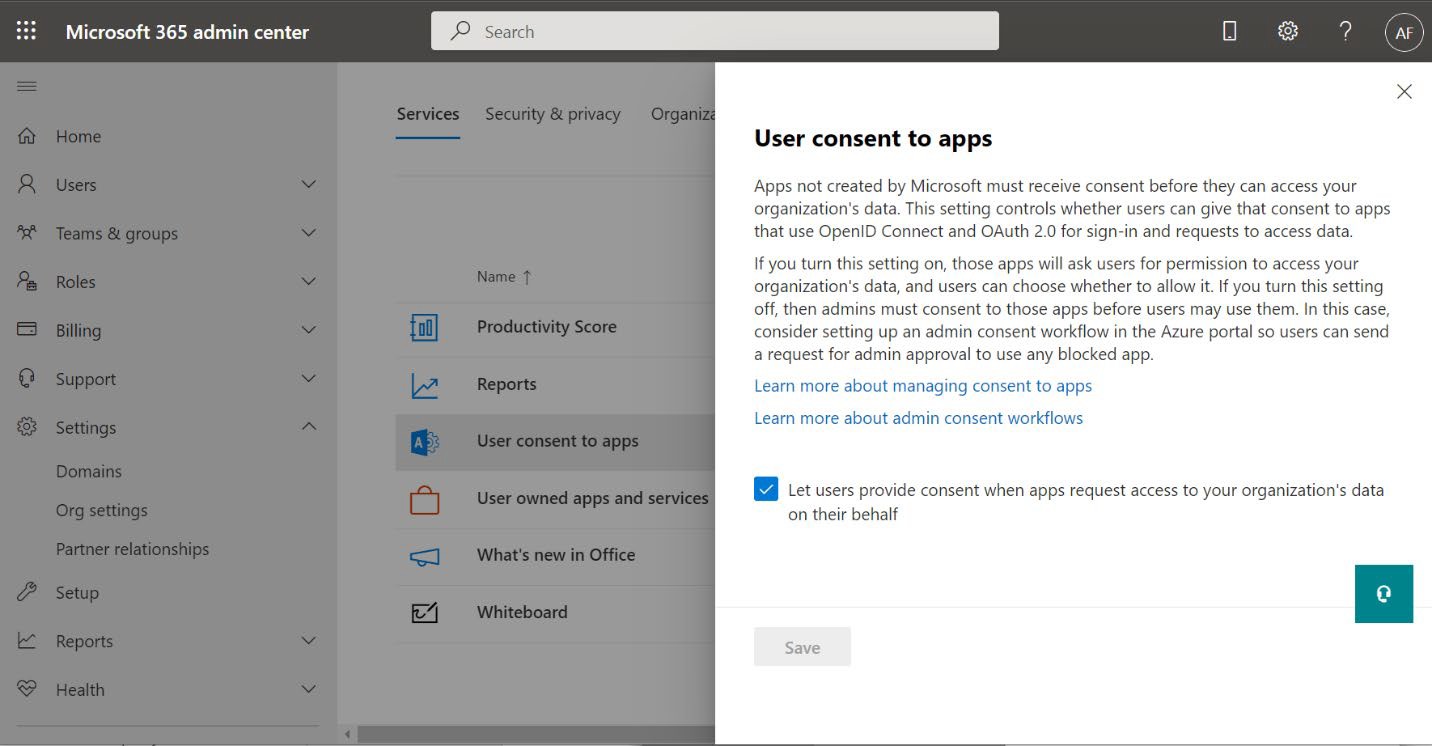
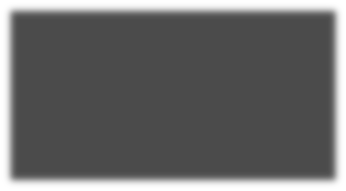
Third-party add-ins and applications for Office 365 may sometimes prompt end users to

consent to granting access to Office 365. Below is an example when activating an Outlook add- in called Adobe Sign (a popular app for electronic signatures):

© Copyright 2019-2022, Azure AD

AZURE AD

24



The reason this is risky is because phishing emails may contain links to malicious apps that trigger this type of workflow, asking the user to grant permissions to their Office 365 data. And this means the attackers would not even require a username and password to get in at all (because they would have an OAuth token granted to them by the already authenticated user).

We have three options to better manage this behavior:

1.

2.

3.

Disable consent to applications requesting permissions

Constrain or limit consent to low permissions from trusted publishers Set up an admin consent request approval workflow

Option 1. Disable app consent

Now it *is* possible to prevent users from being able to consent to these requests in the first place. Navigate to the Microsoft 365 admin center, find **Settings > Org settings** and then find

**User consent to apps**. Clear the checkmark box for ***Let users provide consent when apps***

***request access to your organization’s data on their behalf***.

Click **Save**.

Although this is the easiest way to remove the risk, users will not be able to integrate with third- party apps in this configuration! If you still want to add applications and allow integrations, this would require an administrator to manually complete the process each time ([see this article for](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent) [more details](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent)). For an administrator, going through the consent request process will trigger

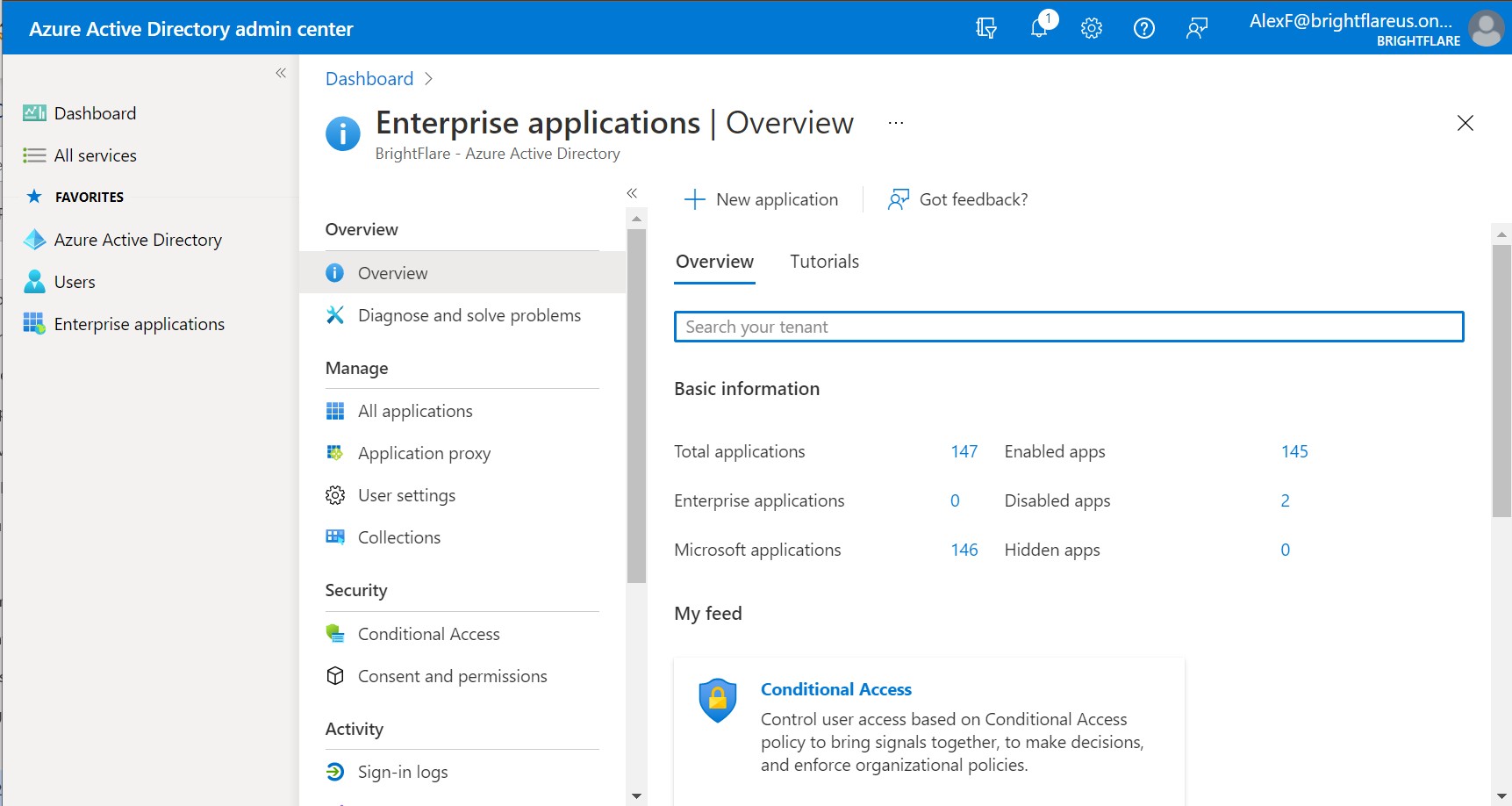
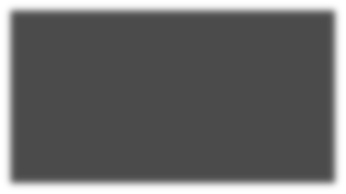
consent for the entire organization (rather than just one user).

© Copyright 2019-2022, Azure AD

AZURE AD

25

Clear this checkbox to disable user app consent outright.



Option 2. Limit app consent

We also have the option to *limit* a user’s ability to consent to application permissions requests. We can accomplish this from the [Azure AD admin center;](https://aad.portal.azure.com/) navigate to **Enterprise applications >**

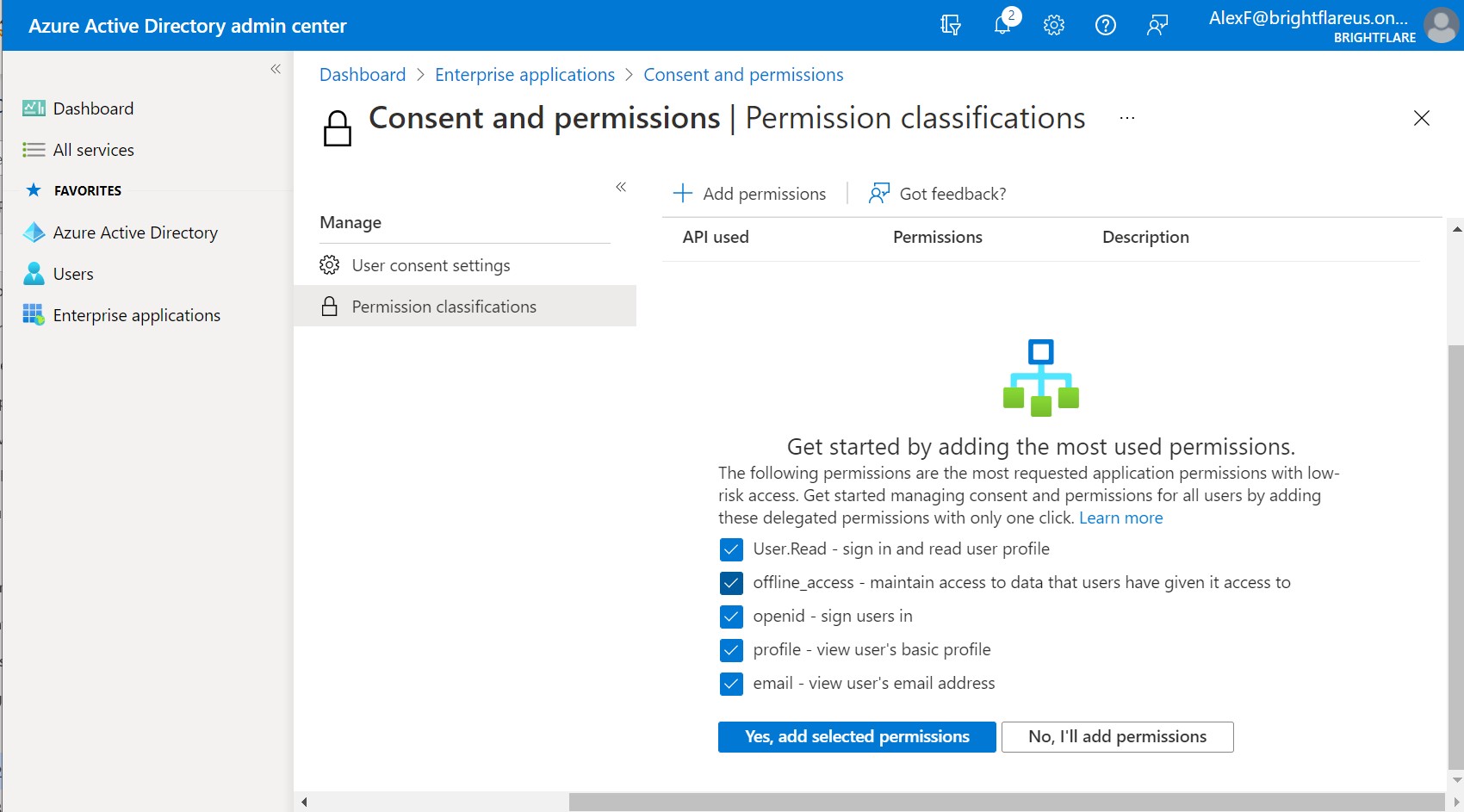
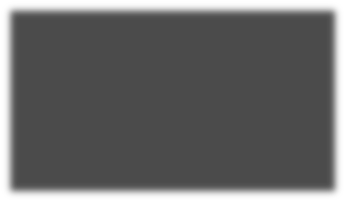
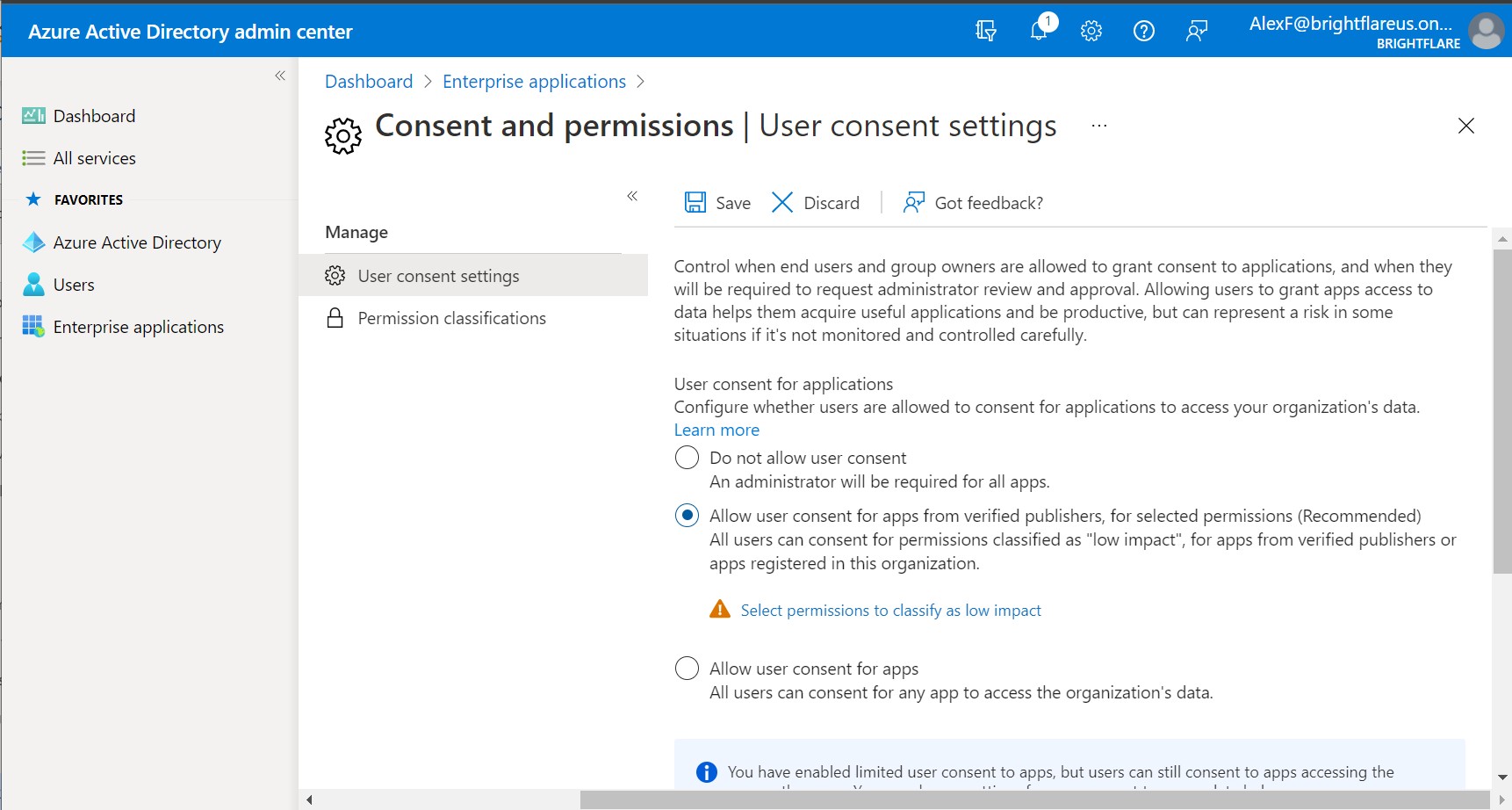
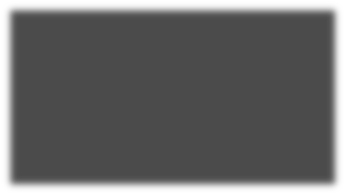
**Consent and permissions**.

To implement this option, select the middle option: “**Allow user consent for apps from verified publishers, for selected permissions (Recommended)**.” Click **Save**.

© Copyright 2019-2022, Azure AD

AZURE AD

26

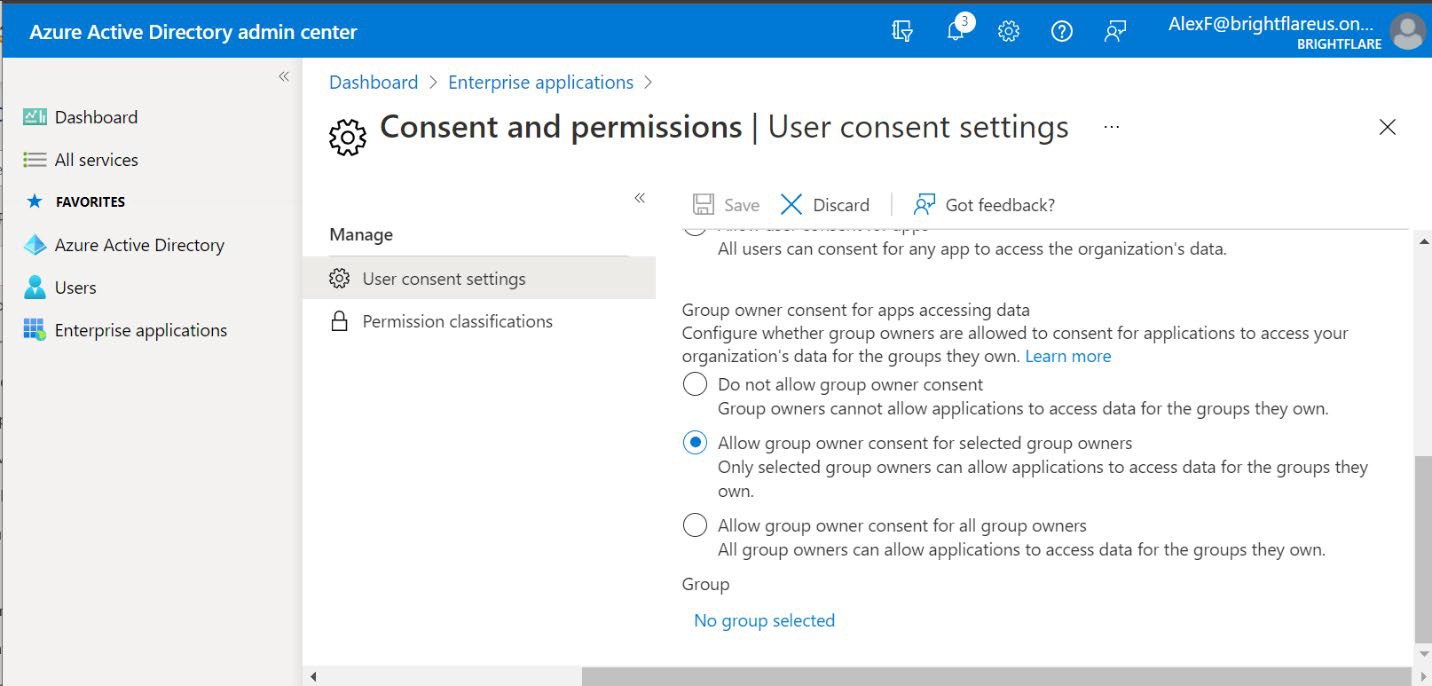
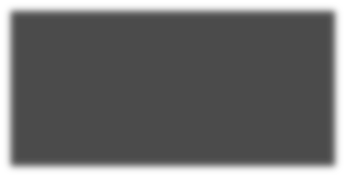


You should also visit the **Permissions classifications** page to set the permissions that are classified as “low” impact.

© Copyright 2019-2022, Azure AD

AZURE AD

27



All you have to do for a minimum acceptable configuration is to select all the checkboxes on this page to allow the most commonly requested low-impact permissions, and then click on the button: **Yes, add selected permissions**.

You can also manage permissions requests for group owners, back on the **User consent settings** page (scroll down to find the group settings). In this case we can restrict *who* is allowed to consent to permissions requests for groups. Your options are: turn it off for everyone, turn it

on for some people, or turn it on for all people.

Some organizations choose to restrict who is allowed to even create Microsoft 365 Groups; if that describes your organization, then you can choose **Allow group owner consent for selected group owners**, and leverage the same security group that you use to manage group creation again here.

If your organization is taking a “closed ecosystem” approach with strong compliance boundaries and a policy that says employees should keep company data in Microsoft 365, then you would most likely select the first option, **Do not allow group owner consent**.

Option 3. Admin consent request workflow

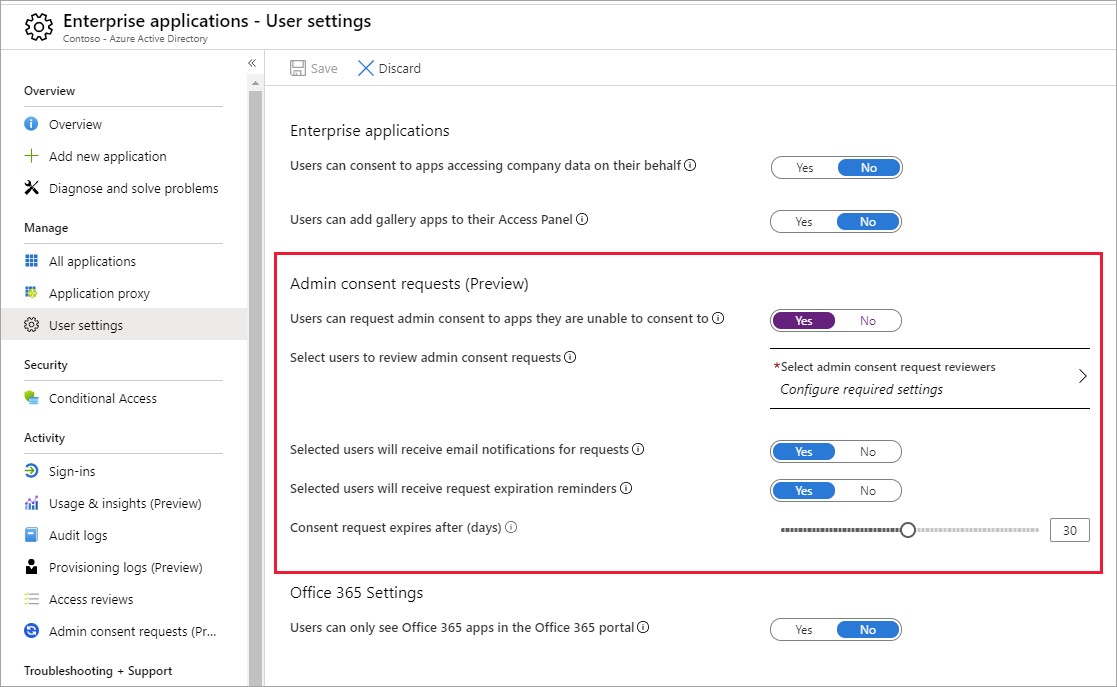
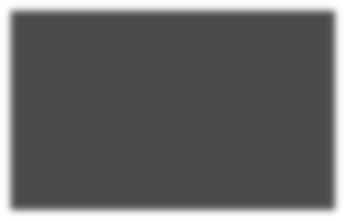
The last option can be combined with either of the above two options. Here we enable an “approval process” where admins can review and then approve requests when users attempt to add applications. Set this up in the **Azure AD admin center** under **Enterprise Applications >**

**User Settings > Admin consent requests**.

© Copyright 2019-2022, Azure AD

AZURE AD

28



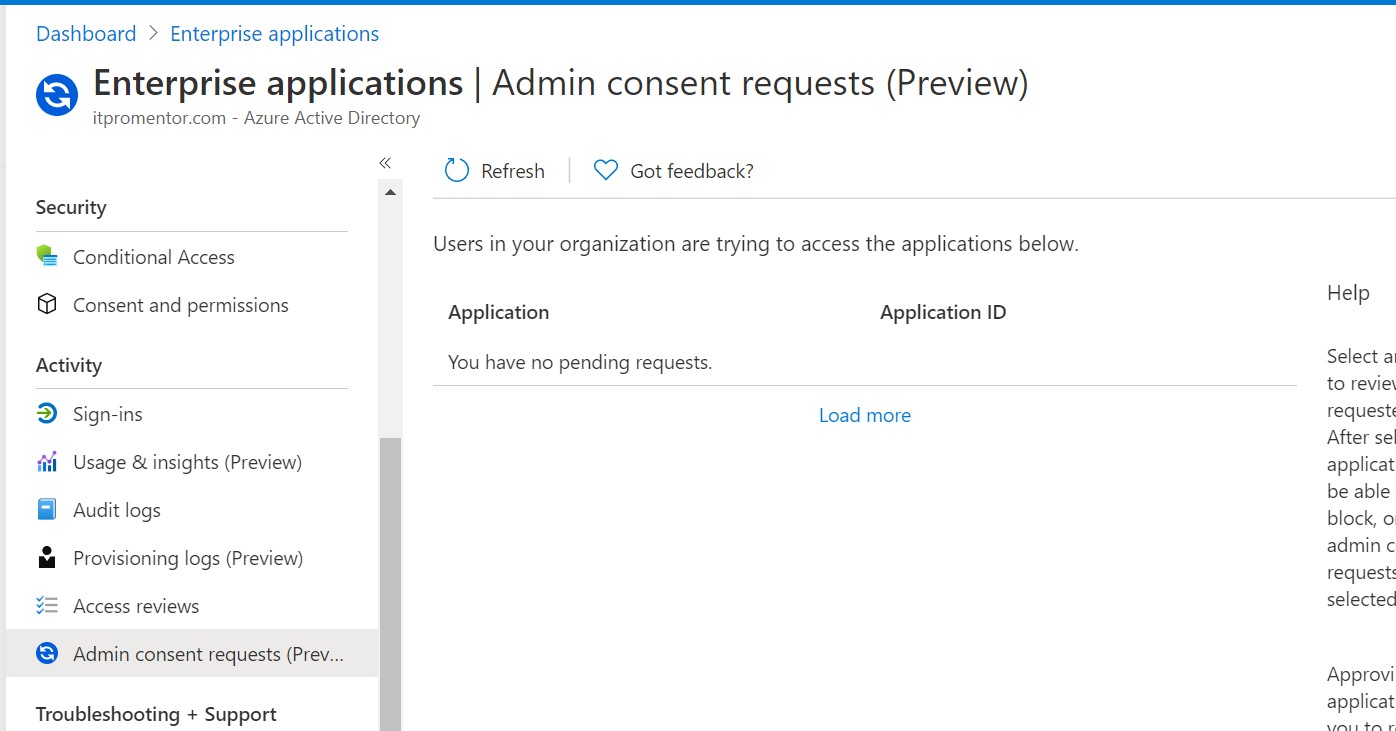
Using this solution, the administrator would be notified when an end user requests permissions for a new application. The designated application administrator would then need to go to the Azure AD admin portal, and consent to every “legitimate” app that users wanted to add. This is done from the Azure AD admin center under **Enterprise Applications > Admin consent**

**requests**.

© Copyright 2019-2022, Azure AD

AZURE AD

29



recommend configuring Admin consent requests. However, another alternative to administratively gating self-service apps is to simply monitor and alert on suspicious OAuth apps, using **Microsoft Cloud App Security**. This product is included with Microsoft 365 E5, Enterprise Mobility + Security E5, Microsoft 365 E5 Security, and is available as a standalone

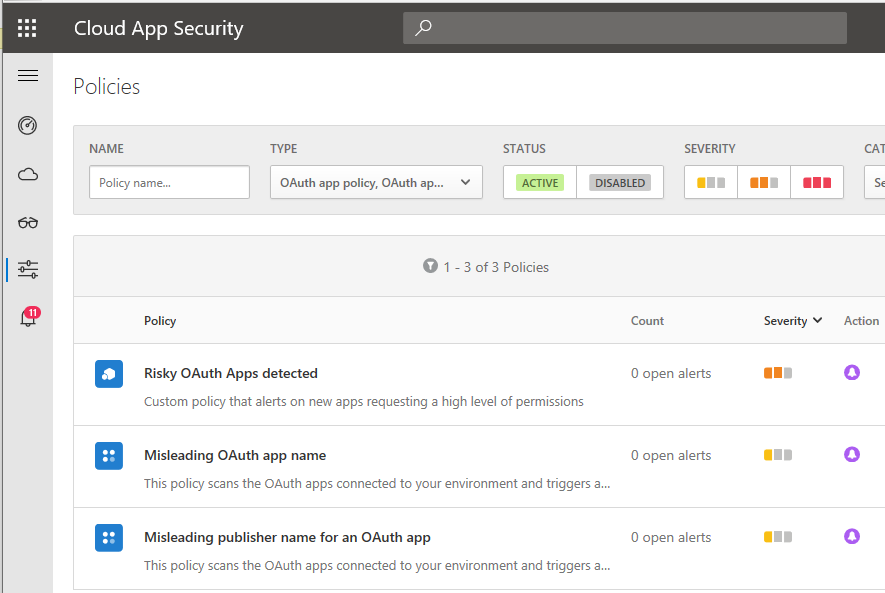
subscription.

© Copyright 2019-2022, Azure AD

AZURE AD

30

Requests that end users make would show up here.



Several alert policies are included out of the box to assist with the management of OAuth apps (e.g. Misleading publisher, Misleading OAuth app name, etc.). You can also create custom rules to watch apps that request a high permission level.

* Restrict guest access and configure external collaboration

Guest access and invitation settings should be reviewed and set as desired by the organization. Find these settings under **External identities > External collaboration settings**.

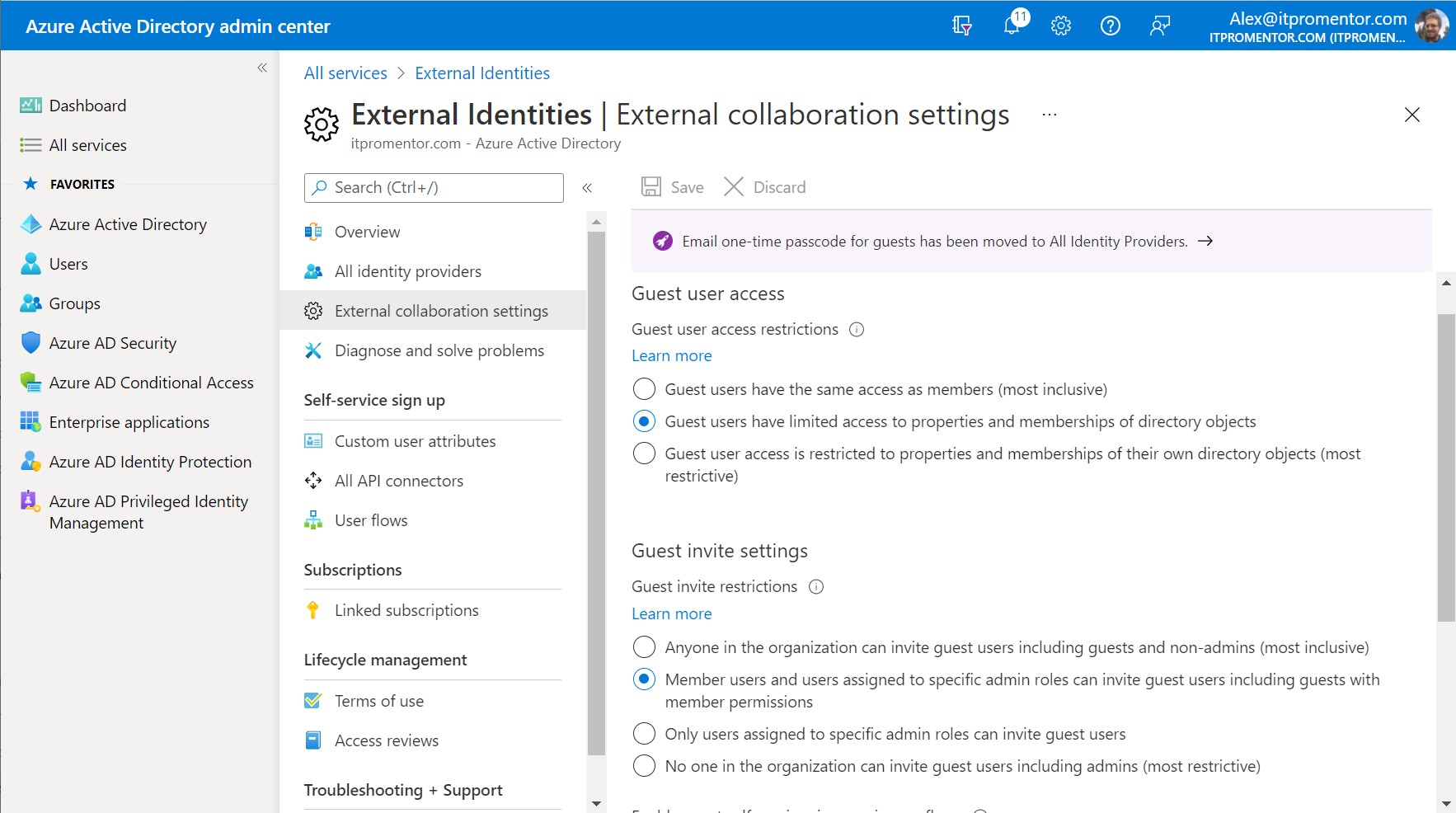
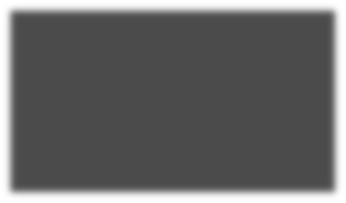
For example, many organizations are comfortable with their own members being able to invite guests to collaborate, but rarely do they feel as comfortable with the idea of guests being able to turn around thereafter and invite new guests.

You can also *limit* the visibility of guests so that they do not see as much information about other members and groups within the organization. My own selections are depicted below.

© Copyright 2019-2022, Azure AD

AZURE AD

31



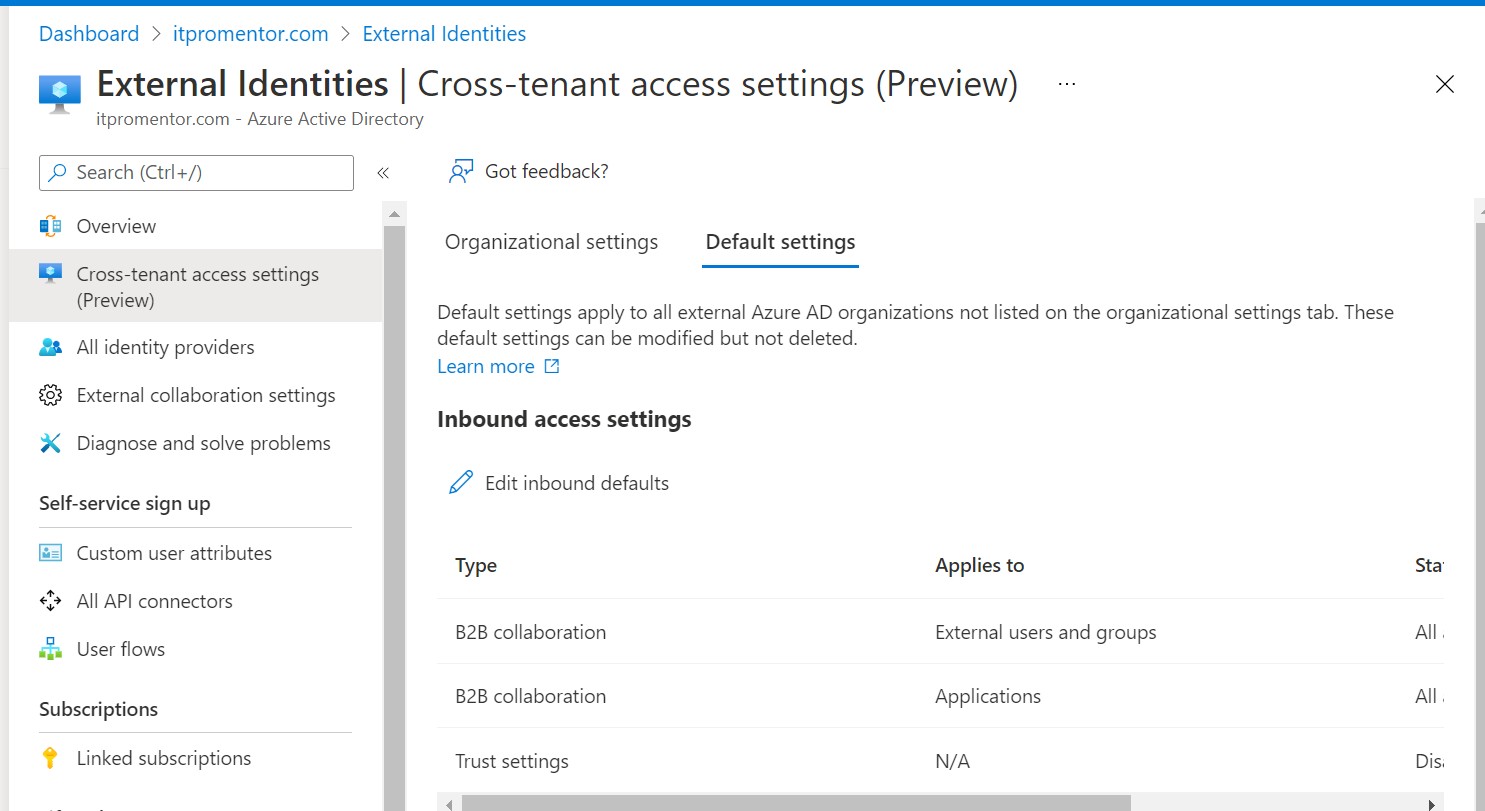
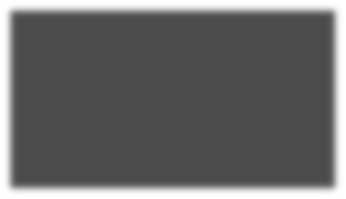
Note that you can also enable self-service sign-up options or even allow invitations to be restricted by domain. Again, these are not IT decisions, but rather decisions that the business should make based on their unique needs for collaboration. The only way to implement a “wrong practice” here is by not discussing these options with the appropriate stakeholders in the business.

Now move to **All identity providers**. Consider **Enable Email One-Time Passcode for guests** as well—this makes it easier to invite guests who do not already have a Microsoft account.

© Copyright 2019-2022, Azure AD

AZURE AD

32



This should be enabled by default now for new tenants, but you should enable it if it is not already on older tenants.

* Trust claims from other Azure AD tenants

In the past, if you wanted to enforce controls like MFA for guests, the experience was sub- optimal, because those users would be “double prompted” for MFA. One to sign-in to their own tenant, and once again to sign into yours. Now it is possible to trust claims from other organizations in Azure AD.

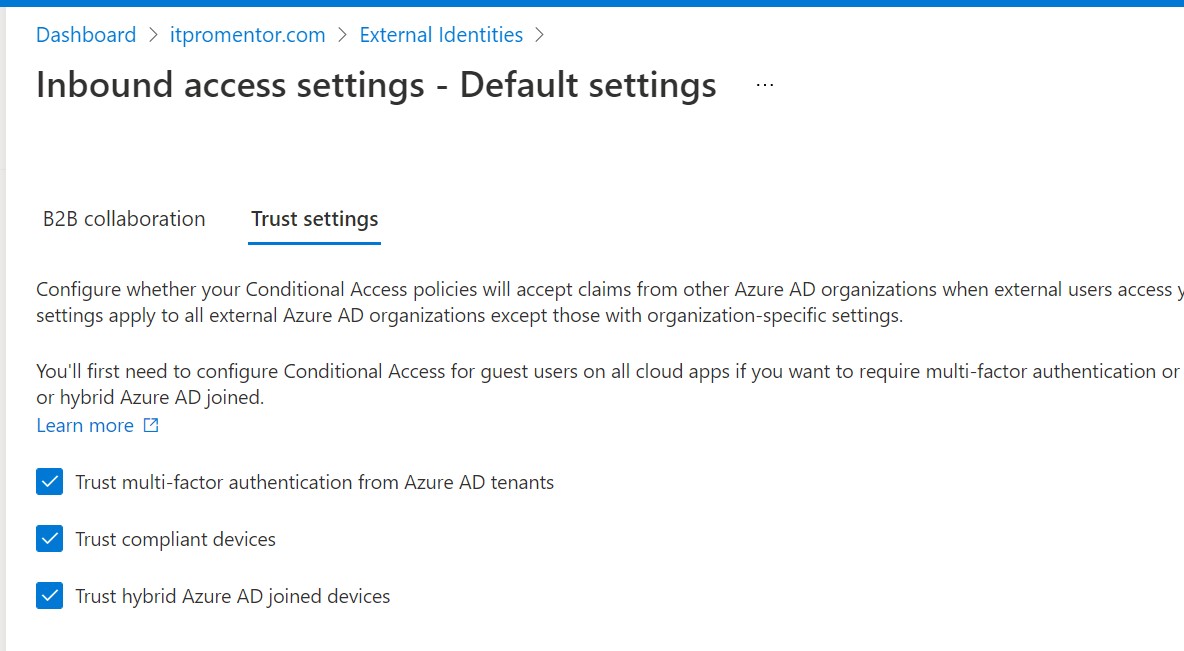
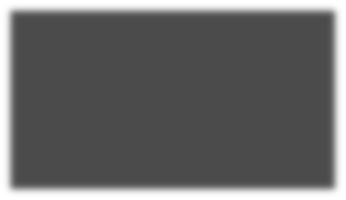
Navigate to **External Identities > Cross-tenant access settings**. Go to **Default settings** and find **Edit inbound defaults**.

Then click on **Trust settings**, and find the options to **Trust multi-factor**…, **Trust compliant devices**, and **Trust hybrid Azure AD joined devices**.

© Copyright 2019-2022, Azure AD

AZURE AD

33



These settings will allow you to deploy Conditional access policies that target guests and external users, and which require either MFA or corporate managed devices (that is, managed by the guest’s organization, not your organization).

* Configure SSO for Enterprise applications

There is a lot of power in this feature, and often advocate for people to start using it more. Even if you do not go as far as configuring Single Sign-On, just the exercise of assigning apps to users and groups is valuable, since you will have a better overall picture and inventory of the apps in your organization.

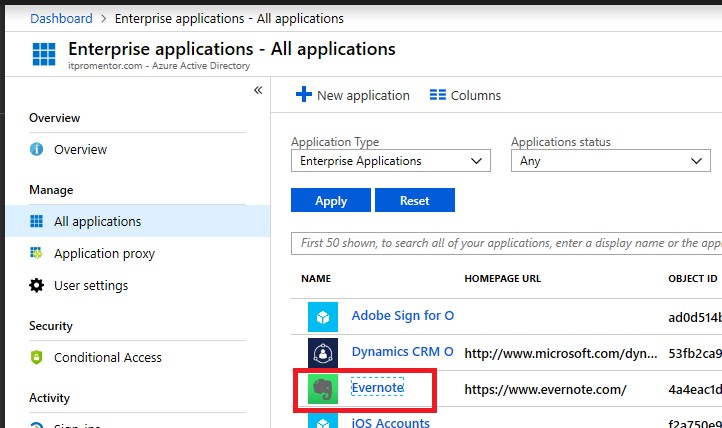
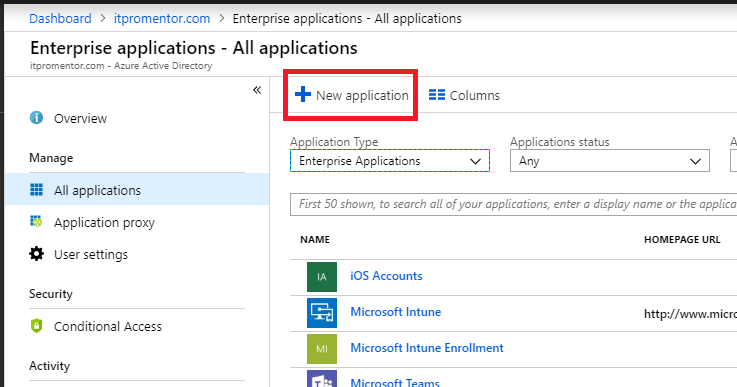
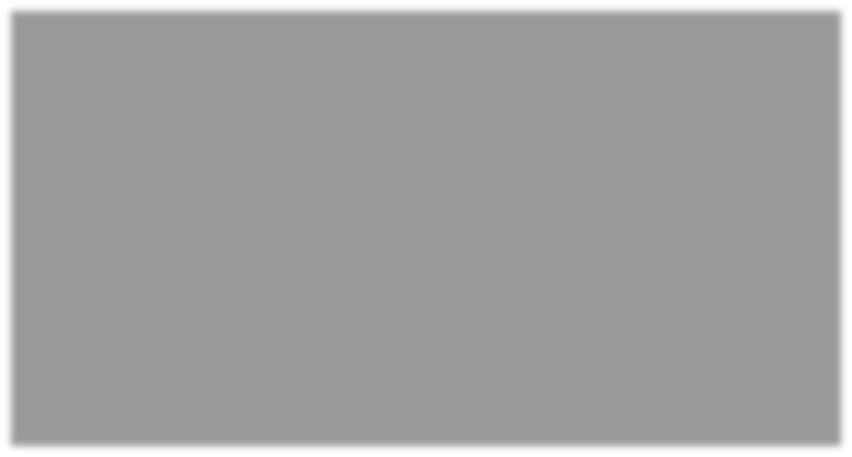
Once you *know* what you have, then it is much easier to take steps to *protect* the associated assets. If you need help identifying apps to begin with, look to your management tool to identify installed software packages, and also consider using [Cloud app discovery.](https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery)

To get started go to Azure Active Directory, find **Enterprise Applications > All applications**. Click **New application**. There a few thousand applications now available in the app gallery.

© Copyright 2019-2022, Azure AD

AZURE AD

34



By way of example only, will search for and add an application from the gallery—in this case

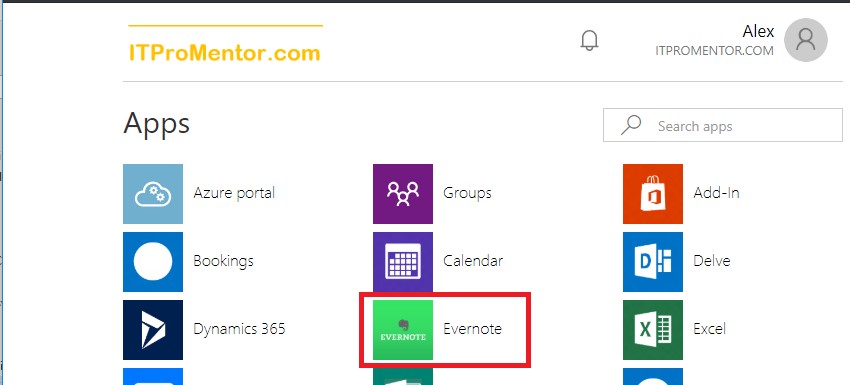
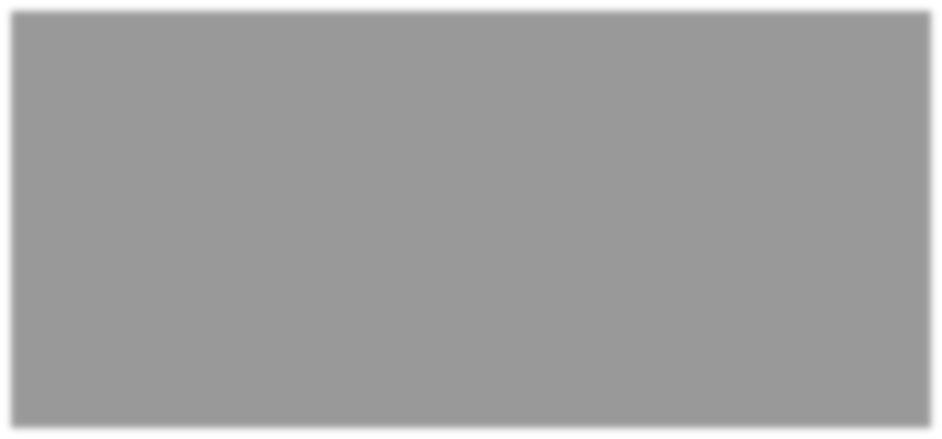
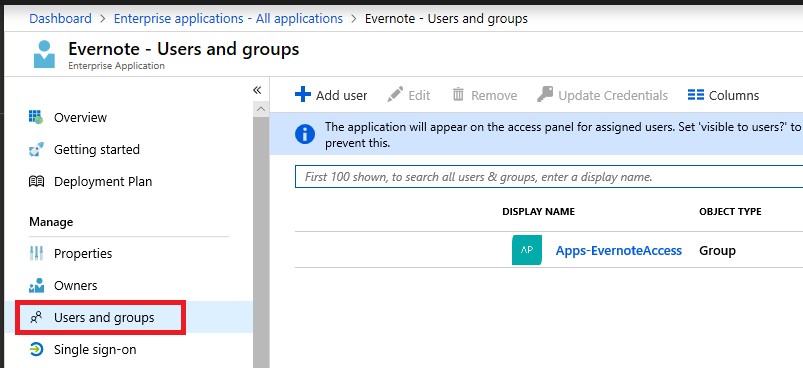
*Evernote*.

Next, can assign the application to individual users, or to a security group which have created for this purpose. Click the application and find **Users and groups** to make your assignments.

© Copyright 2019-2022, Azure AD

AZURE AD

35

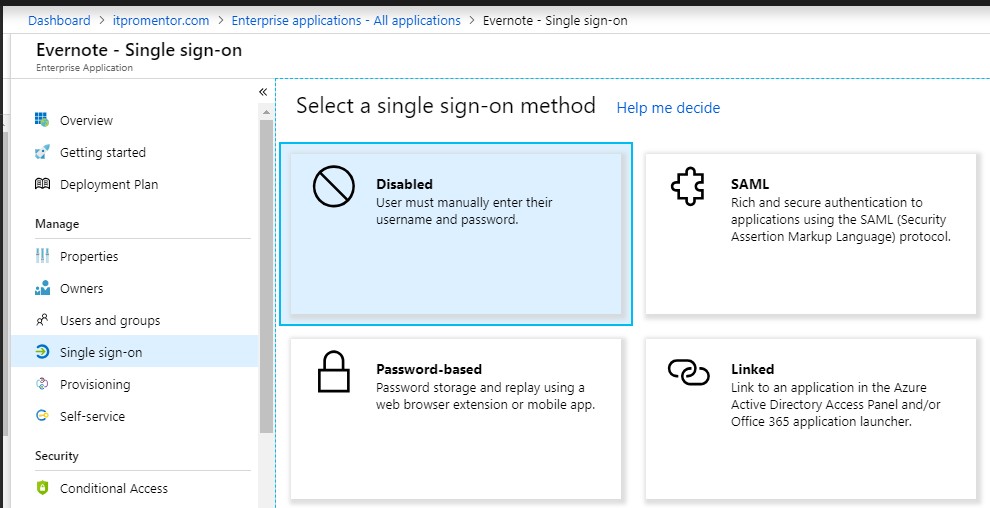
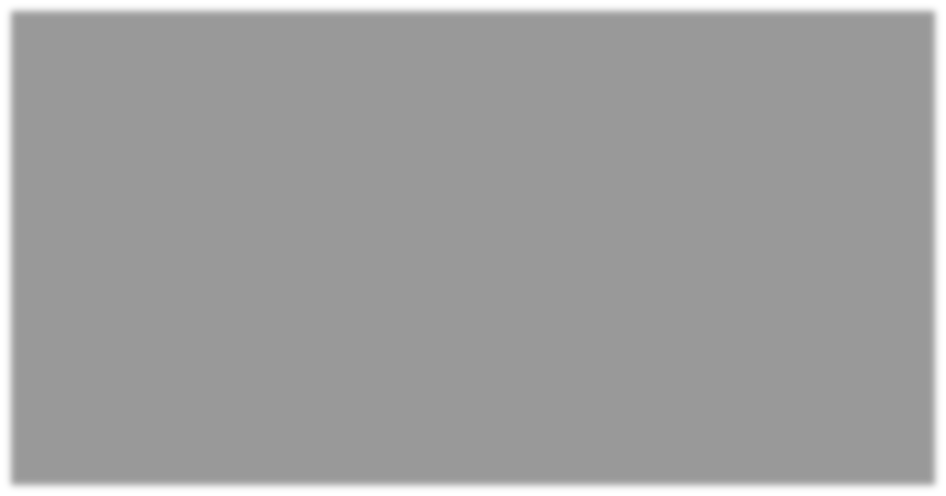
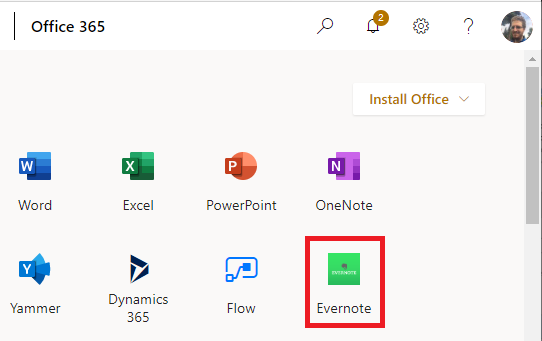


After you have configured your apps and assigned them to groups, your users will be able to access the applications via the Azure AD access panel located at [https://myapps.microsoft.com](https://myapps.microsoft.com/)

© Copyright 2019-2022, Azure AD

AZURE AD

36



Enterprise apps can also be displayed in the app launcher for Office 365.

Now find the **Single Sign-On** blade within the application. Not all applications will support “true” single sign-on (SSO), but almost any app will allow the user to store their credentials within the Azure AD portal (similar to LastPass, if you are familiar with that concept). The various

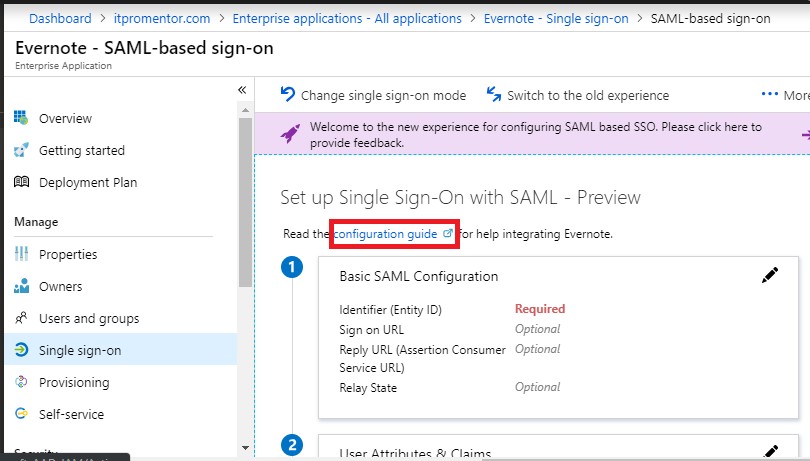
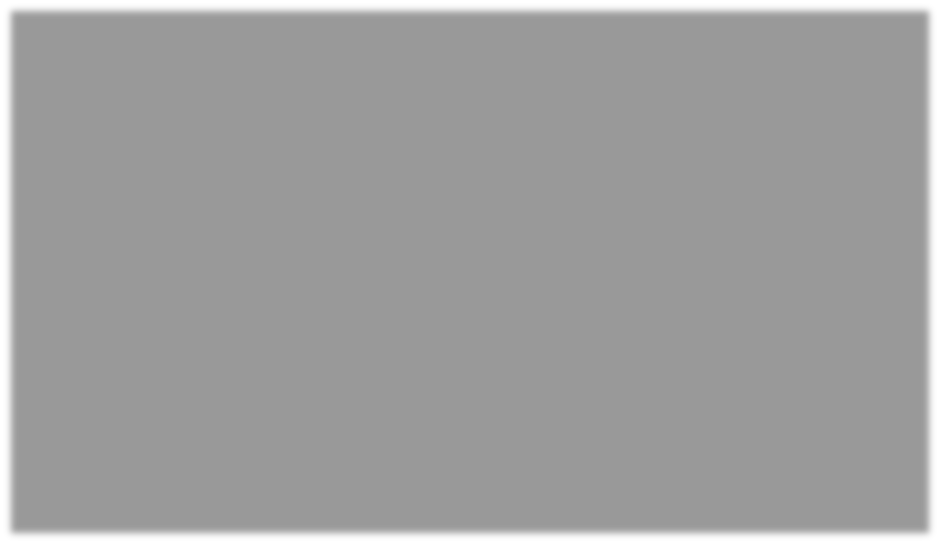
SSO methods are depicted in the following screenshot, and explained below.

**SAML** is the option you want. If the app supports SAML (Security Assertion Markup Language), that means it will be capable of “true” SSO, where Azure AD becomes the app’s Identity

© Copyright 2019-2022, Azure AD

AZURE AD

37



Provider, and all authentication requests are logged against Azure AD—whether they come in via the app portal, or not. This is the most secure option and recommended wherever possible.

The security benefits of SSO are just too great to ignore, since you can reduce the number of identities you manage and centralize the security logs in Azure AD. Plus, you can apply things like Conditional Access and MFA to the logon requests as well, just as you do with the Microsoft apps. None of this is that hard to do, so do not be afraid of it.

Every app is a little bit different in terms of its deployment, although they all have similarities. Here are some basic guidelines can give you: Microsoft links to a **configuration guide** for

many common gallery applications.

In almost all cases where SAML is available, you will need to provide Azure AD and the third- party application with some URLs, certificates and/or XML files, so that each side can understand and talk with the other. Note that sometimes certain entries are optional. Microsoft and/or

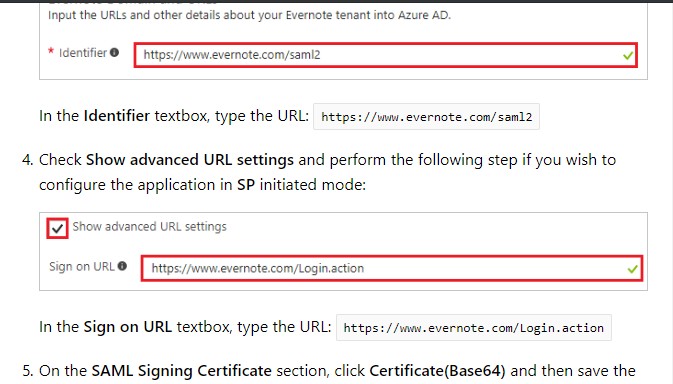
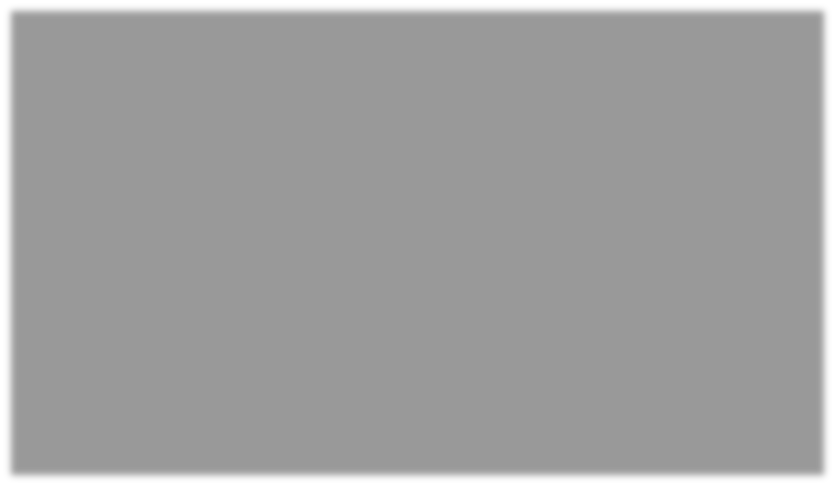
third-party vendors will likely have support documentation available, as pictured here in the case

of Evernote.

© Copyright 2019-2022, Azure AD

AZURE AD

38



It is difficult to express just how important this Enterprise Application feature could be for your organization or practice. Even if you cannot configure true SSO with SAML to every one of your

applications, just the fact that you can *track* application assignments to users alone is huge.

Items of Optional Importance

* Configure Company branding

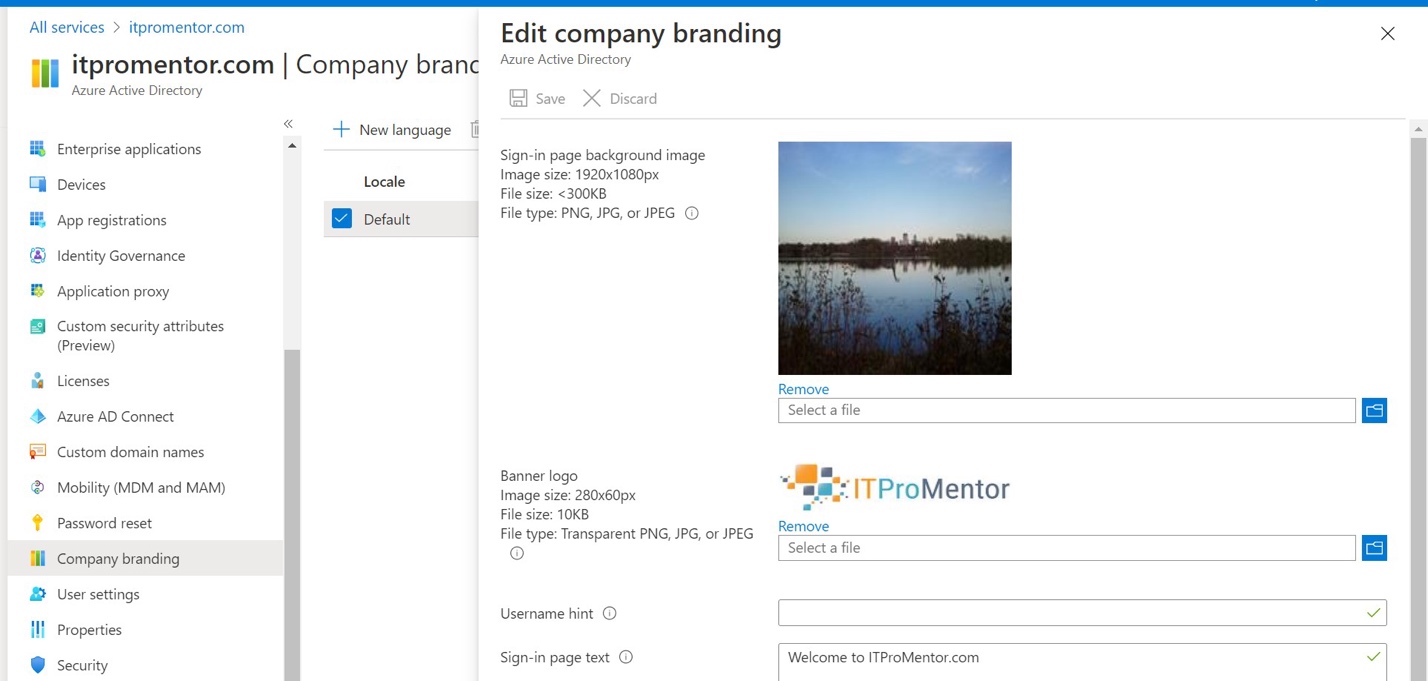
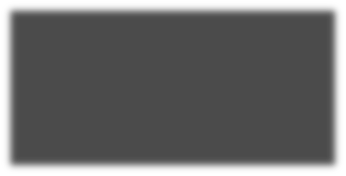
Company branding is usually viewed as something highly optional and purely aesthetic, but believe it has an impact on security, too. The reason being: many phishing campaigns will send users to fake login pages that mimic the popular cloud services like Office 365. Therefore, if you customize the login experience with your brand, it is less likely that users will fall for the generic “look-alikes.” However, note that some targeted phishing campaigns out there will also leverage

your branding elements, so it is not fool-proof by any means.

© Copyright 2019-2022, Azure AD

AZURE AD

39



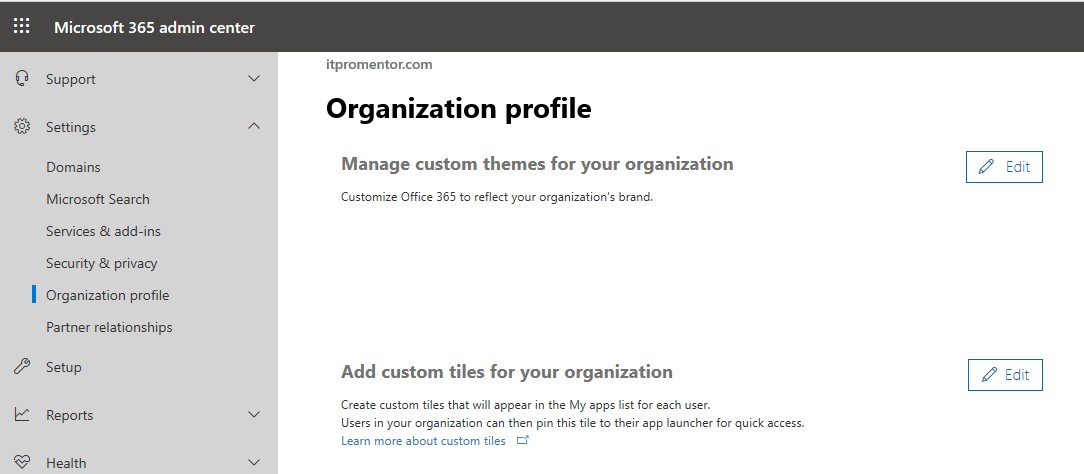
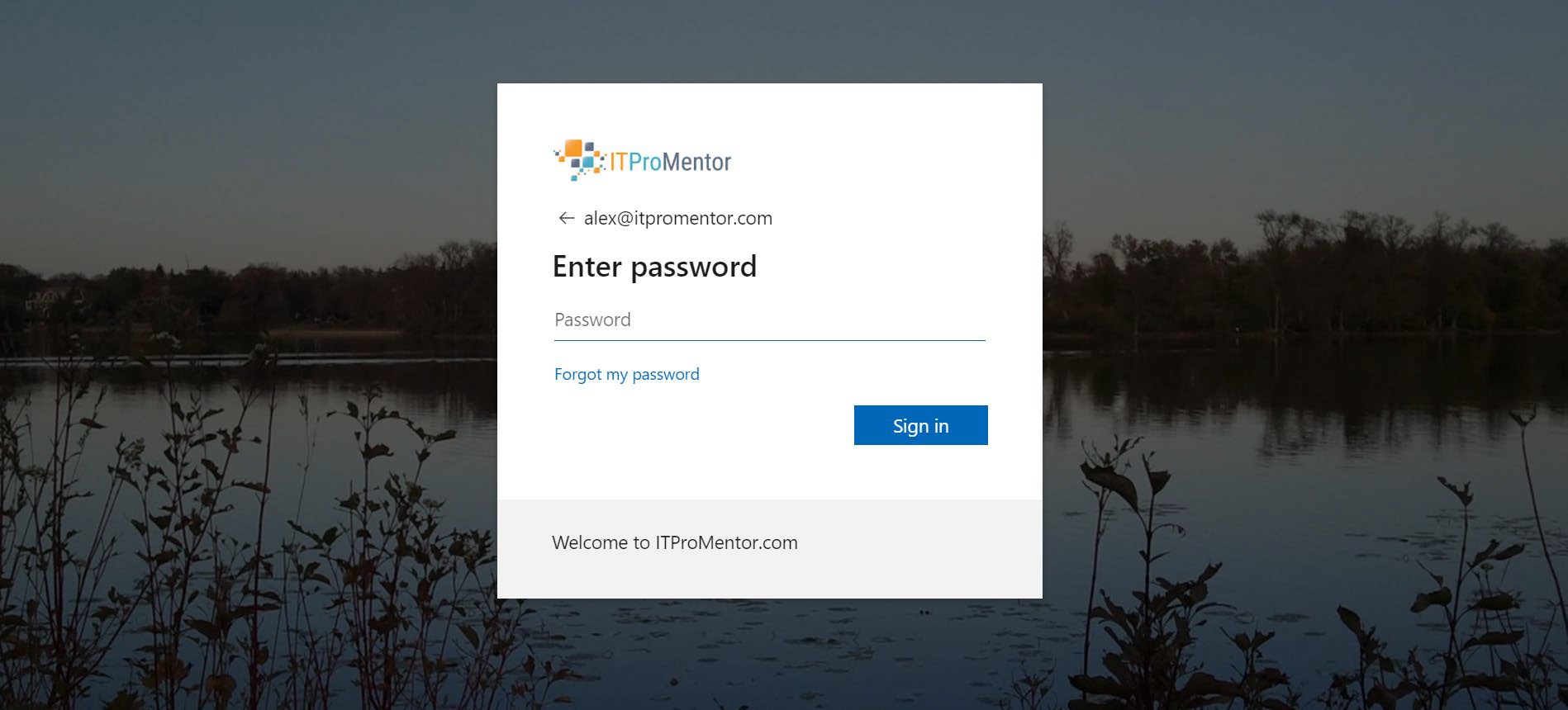
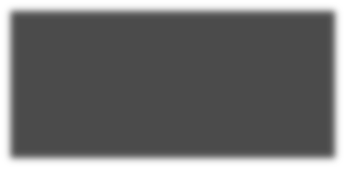
From the Azure Active Directory admin center, click **Azure Active Directory** and scroll down to find the blade for **Company branding**. Click **Configure**. will not go through all the options here, but the first two are the most common: *background image* and *banner logo*. By way of example, in the image below, have configured both. After making this change, the Azure AD

sign-in page will feature the new branding.

© Copyright 2019-2022, Azure AD

AZURE AD

40



The logo you upload here will flow though into some other areas (e.g. the application access panel at [myapps.microsoft.com](https://myapps.microsoft.com/)), but there are other branding options in the 365 admin center,

which are used as part of your “theme” in Office 365. **Settings > Organization profile**.

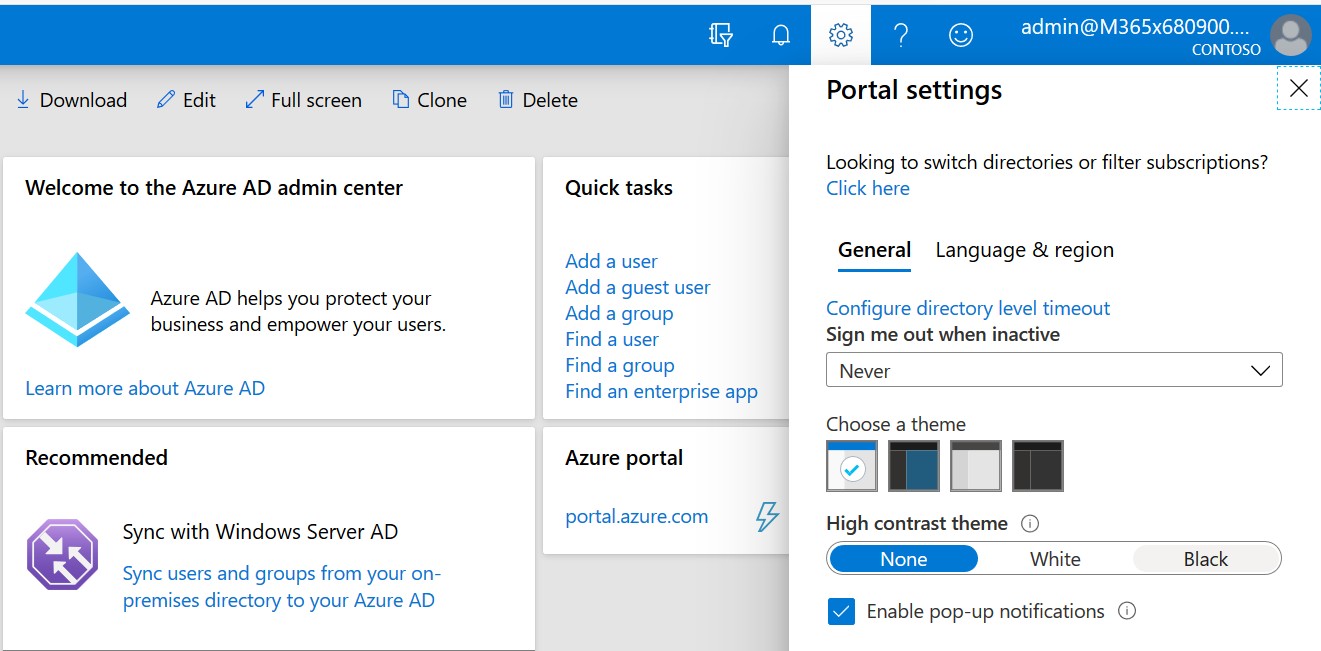
And neither of these customizations will flow through to the branding for encrypted emails —

that is yet another *separate* branding. hope that Microsoft collapses these disparate areas into one single place someday.

© Copyright 2019-2022, Azure AD

AZURE AD

41



* Enable Directory level timeout for the Azure portal

In the upper right corner of the portal, go to **Settings (gear icon) > Configure directory level timeout**. Here you can choose a value to time out the browser session so that it cannot be left open indefinitely when admins are working in the Azure portal.

* Use Administrative Units to delegate admin permissions

Azure AD Administrative Units (AU’s) are only applicable in larger sized environments, typically. They are often compared to Organizational Units (OU’s) in on-prem Active Directory, but it would be a mistake to equate them (AU’s are much more limited in function than OU’s).

The reason you would use Administrative Units is to segment your directory into different “containers” and assign administrative permissions over certain users and groups to different individuals.

For example: Regional administrators who manage users and groups at their respective locations. For the SMB market, where spend most of my time, this is not something we are likely to use. However, some mid-sized or larger orgs may find this helps them to solve for certain issues or regulatory requirements.

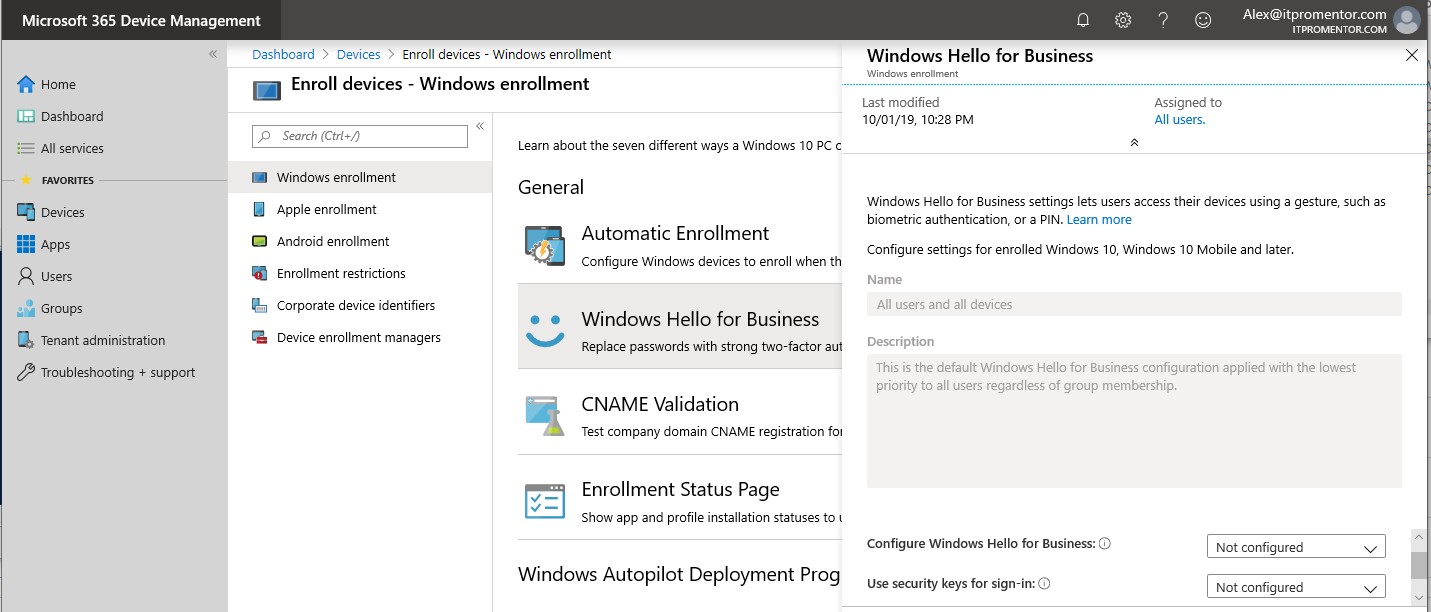
See this article for more details:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

© Copyright 2019-2022, Azure AD

AZURE AD

42



* Considerations for Hybrid Azure AD Join

In hybrid environments where a legacy Active Directory environment is connected to Azure AD via the Azure AD Connect tool, several other setup steps are necessary to complete the richest experience for Microsoft 365 and hybrid device management capabilities.

The links below will describe the steps you need to take to complete the Hybrid Azure AD Join configuration. These steps assume that you are using a *managed* domain, not a *federated*

domain with AD FS. Avoid AD FS if you can and use Password Hash Synchronization instead.

1.

2.

3.

4.

[Install Azure AD Connect](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom)

[Setup Hybrid Azure AD Join (Managed domains)](https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains) [Create GPO to enable auto-enrollment with Intune](https://docs.microsoft.com/en-us/windows/client-management/mdm/enroll-a-windows-10-device-automatically-using-group-policy)

[Enable Windows Hello for Business (Hybrid key trust)](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-key-trust)

Note: It is required to have at least one Windows Server 2016 domain controller in the environment to support Windows Hello for Business with Hybrid Key Trust.

You are not done configuring hybrid until all the above steps are completed. If you are stuck with AD FS, then steps 2-4 may look slightly different for you:

2.

3.

4.

[Setup Hybrid Azure AD Join (Federated domains)](https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-federated-domains) [Federated authentication device enrollment](https://docs.microsoft.com/en-us/windows/client-management/mdm/federated-authentication-device-enrollment)

[Enable Windows Hello for Business (Hybrid certificate trust)](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cert-trust)

If you do not want to configure Windows Hello for Business, then you can also disable it from

**Devices > Enroll devices > Windows enrollment > Windows Hello for Business**.

© Copyright 2019-2022, Azure AD

AZURE AD

43

In general, believe that small businesses should be taking steps toward a “cloud-only” configuration, and not relying on hybrid moving into the future, as this presents more risks and complications than benefits in my opinion. However, if you are stuck on hybrid, recommend

the following (bullet point advice only):

**UPN Matching**: It is best practice to ensure your logon name (UPN) on-premises matches the primary email address, which is used as your sign-in for Microsoft 365. **Password Hash Sync:** is the only right choice, and do not try do something fancier than that. And get rid of AD FS is that is still around. Yuck.

**Password policy on-prem:** Make sure you have a good password policy in place here, or you just end up bringing your crappy practices into the cloud (no bueno). You can improve password security and the end-user experience using [password-](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-writeback) [write back](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-writeback) for self-service password reset, and via enabling [password protection](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises) for on-premises servers.

**Limit the scope of your sync**: Whether you filter via OU, account attributes or both, just do not let the clutter from your on-premises environment come along for the ride. The fewer accounts you must manage, the better.

**Disable any shared accounts**: You should not be signing into shared accounts interactively. Generally speaking, you delegate access to resources (e.g. shared mailbox) to other user accounts, which have “real” people behind them.

**Consider ditching distribution lists**: When you move to Office 365, you may want to get rid of traditional DL’s in favor of Office 365 Groups, which come with a lot more benefits. You need to remove the lists from on-premises AD and re-create them in the cloud as Groups instead.

**Get to know what changes where and when**: Some changes have to be made on- prem (new accounts, name change, new alias, hide from address list, enable archive, etc.) while others, like delegations, forwarding, etc., are still managed in the cloud.

**You still need at least two “cloud-only” global admin accounts**: We covered this.

**There are probably others**: Like said, hybrid is not known for simplicity. But this is a good start.

o

o

o

o

o

o

o

o

o

* Azure AD Premium P2 features or E5

have written this guide to apply broadly—to all major Microsoft 365 bundles from Microsoft 365 Business Premium and Enterprise E3 on up. If you are lucky enough to have a fancy Microsoft 365 E5 subscription with access to Azure AD Premium P2 features, three additional things recommend looking at are:

* + [Identity Protection:](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/enable) Identity protection and the risk-based policy additions to Conditional Access make it possible to protect risky sign-in attempts and user identities that have been identified as at-risk by the Microsoft Intelligent Security Graph.

© Copyright 2019-2022, Azure AD

AZURE AD

44

* [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan) (PIM): Enables you to strip admin privileges and demote those accounts so that they are merely “eligible” for admin access—then [granting](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow) access as needed, on a “Just in Time” basis, and only then for a specific window of time.
* [Access Reviews:](https://docs.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews) Helps you manage the resource access lifecycle; another check and balance to validate that users (both internal and external) who have certain access today do in fact still require it.

© Copyright 2019-2022, Azure AD

AZURE AD

45